Centro Universitário de Brasília - UniCEUB

Faculdade de Ciências Jurídicas e Sociais - FAJS

Marcus Vinicius Rodrigues Padilha

RELAÇÕES INTERNACIONAIS E ESPAÇO CIBERNÉTICO: SISTEMAS DE DEFESA DOS EUA E BRASIL

Brasília

2016

Marcus Vinicius Rodrigues Padilha

RELAÇÕES INTERNACIONAIS E ESPAÇO CIBERNÉTICO: SISTEMAS DE DEFESA DOS EUA E BRASIL

Monografia apresentada como requisito para conclusão do curso de Bacharelado em Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais do Centro Universitário de Brasília - UniCEUB.
Orientador: Prof. Gabriel Mattos Fonteles.

Brasília

2016

Marcus Vinicius Rodrigues Padilha

RELAÇÕES INTERNACIONAIS E ESPAÇO CIBERNÉTICO: SISTEMAS DE DEFESA DOS EUA E BRASIL

Monografia apresentada como requisito para conclusão do curso de Bacharelado em Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais do Centro Universitário de Brasília - UniCEUB.
Orientador: Prof. Gabriel Mattos Fonteles.

Brasília, de de 2016.

Banca Examinadora

_____

Prof. Gabriel Mattos Fonteles

Orientador

_____

Examinador (a)

_____

Examinador (a)

Dedico este trabalho aos meus pais, irmãos, avós e madrinhas, por todo incentivo e apoio incondicional.

AGRADECIMENTOS

Em primeiro lugar agradeço à minha família. Aos meus pais, Leopoldo André e Luciana que com muito amor e sacrifício se dedicaram integralmente ao sucesso meu e dos meus irmãos. Aos meus avós, Anna Lúcia, Joaquim e Dida, e minhas madrinhas, Dadá e Zeda, que junto com meus pais não mediram esforços para a minha formação cívica e acadêmica. Aos meus irmãos, André Luis e Natasha, pelo companheirismo e inspiração.

Faço um agradecimento especial ao meu orientador Gabriel Fonteles, por ter acreditado nesse trabalho, pela dedicação e paciência em todas as etapas do desenvolvimento da pesquisa. À professora Renata, que desde o primeiro semestre esteve sempre disposta a ajudar e em nenhum momento deixou de ouvir aos alunos. Ao professor Fred e seu papel essencial no curso de Relações Internacionais, sempre em busca do máximo crescimento acadêmico de seus alunos. À todos os outros professores do curso de Relações Internacionais e seu papel essencial na formação de cada um dos alunos. Ao UniCEUB e todos os seus colaboradores.

Agradeço à Thaís, minha namorada e companheira, por todo apoio e paciência no desenvolvimento desse trabalho. Ao Mateus Klitzke por tudo o que passamos juntos e por estar sempre ao meu lado nessa aventura que foi a faculdade. À Juliana Tomazini, Kleber Tejera e todos os outros amigos e colegas de faculdade, por todos os desafios enfrentados juntos. Ao Danilo pelos 20 anos de amizade e por estar sempre presente. Ao Edoardo Lazzaretti pelo companheirismo. Aos amigos do Sigma, Henrique, Felipe, Igor e Isadora, que foram essenciais para que eu chegasse até aqui.

A todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

"Basta ser sincero e desejar profundo, você será capaz de sacudir o mundo"

(Raul Seixas)

RESUMO

Este trabalho tem como objetivo apontar como os Estados Unidos da América e o Brasil vêm se preparando para lidar com as ameaças do espaço cibernético. Pelo aspecto recente do assunto nas Relações Internacionais o primeiro passo será uma introdução ao tema, uma análise do que já foi produzido na academia nacional e internacional e as principais teorias utilizadas no desenvolvimento das pesquisas. Por meio de uma análise histórica dos principais ataques cibernéticos serão analisados os tipos de ataques e suas consequências. Por fim a análise de como os Estados Unidos e o Brasil estão lidando com as ameaças e uma comparação entre as principais semelhanças e diferenças das políticas dos dois países.

Palavras-chave: Espaço Cibernético. Brasil. Estados Unidos. Espaço cibernético. Segurança cibernética. Escola de Copenhagen. Securitização. Militarização.

ABSTRACT

This study aims to analyze how the United States and Brazil are preparing to deal with the threats of cyberspace. Due to the recency of the subject in International Relations the first step will be an introduction to the subject, an analysis of what has been produced in national and international academia and the main theories used in the development of the researches. Will be made a historical analysis of the major attacks and their consequences. Finally the analysis of how the United States and Brazil are dealing with the threats and a comparison between the main similarities and differences between the policies of both countries.

Keywords: Cyberspace. Brazil. U.S. Cyber Security. Copenhagen School. Securitization. Militarization.

SUMÁRIO

INTRODUÇÃO

Nós vivemos em um mundo conectado. O acesso ao espaço cibernético está cada vez mais barato, menos complicado, mais difundido e mais necessário. Somente nos últimos 10 anos, o acesso à internet cresceu em mais de 2 bilhões de pessoas no mundo. A internet alterou drasticamente a forma como consumimos informação e como interagimos com atividades corriqueiras. Transações bancárias, videoconferências, notícias, correio, filmes e compras são exemplos dessas atividades que hoje podem ser realizadas por meio da internet através de um simples aparelho celular e em um curto espaço de tempo (USA, 2015).

Estados e empresas não ficam de fora dos efeitos do espaço cibernético. Transações financeiras e até mesmo as movimentações de forças militares já dependem do espaço cibernético. Sistemas de infraestrutura crítica, como usinas de energia e o controle de tráfego aéreo estão conectados e dependem da integridade e do bom funcionamento das redes. As mesma qualidades que levaram à internet à uma grande expansão resultam na emergência de uma nova ameaça, a cibernética. O espaço cibernético se tornou um novo método de realização de ataques e espionagem, tanto por Estados, quanto por atores não estatais. O aumento dos ataques cibernéticos representa uma tendência preocupante para as Relações Internacionais, já que quanto mais dados sigilosos e críticos são armazenados *online*, cada vez maiores são as consequências desses ataques.

Um exemplo da atual evidência do espaço cibernético como item relevante na agenda para as Relações Internacionais está na atenção que é dada ao assunto nas eleições presidenciais de 2016 dos Estados Unidos. No primeiro debate transmitido entre os candidatos Hillary Clinton e Donald Trump, os ataques cibernéticos foram o primeiro tópico a ser debatido quando o assunto passou para a área de segurança nacional. Clinton descreveu a guerra cibernética como um dos principais desafios a ser enfrentado pelo próximo presidente americano. O candidato republicano, Donald Trump, declarou que o conflito cibernético é um grande problema com o qual os Estados Unidos não está sabendo lidar (FORTUNE, 2016).

O espaço cibernético possui características únicas. Uma delas é o anonimato, que muitas vezes torna impossível o rastreio da origem de um ataque e consequentemente uma retaliação. Outra característica é a diferença entre os investimentos necessários para atacar e para se defender no espaço cibernético. Enquanto qualquer pessoa com acesso à um computador básico e com o conhecimento necessário pode realizar ataques cibernéticos contra um Estado, um Estado precisa investir milhões de dólares para criar uma rede de defesa segura, capaz de proteger seus documentos, sistemas de infraestrutura e ainda ter a capacidade de rastrear e retaliar.

A liberdade do espaço cibernético tem se mostrado uma forte arma para grupos terroristas, mais recentemente há uma crescente preocupação com o modo como o Estado Islâmico (ISIS), tem utilizado o espaço cibernético para propagar suas ideias, recrutar e compartilhar seus feitos. As mídias sociais facilitaram o recrutamento do ISIS, pelo menos 30 mil combatentes estrangeiros, de 100 país diferentes foram atraídos para os campos de batalha da Síria e Iraque. O surgimento de novos núcleos do Estado Islâmicos em países como Líbia, Afeganistão, Nigéria e Bangladesh também está diretamente ligado à expansão cibernética do grupo (BROOKING; SINGER, 2016).

O primeiro capítulo deste estudo consiste em um apontamento da literatura das Relações Internacionais em relação ao espaço cibernético, assim como uma exposição dos principais termos da área. Foram analisadas notícias, documentos, livros e artigos tanto da academia brasileira quanto da estrangeira. As ideias dos autores foram expostas e comparadas, houve também um levantamento das principais correntes de pensamento que norteiam as análises das relações e políticas internacionais no espaço cibernético.

O segundo capítulo aborda o relato histórico dos principais ataques cibernéticos envolvendo Estados e as suas consequências. Os três ataques analisados foram escolhidos de acordo com a sua relevância para o Sistema Internacional, com base nos atores envolvidos, o momento em que ocorreram e a sua efetividade. A análise ocorre em ordem cronológica, começando com o ataque à Estônia em 2007, seguido pelo ataque à Geórgia em 2008 e o Stuxnet em 2010. O caso do Stuxnet é até

hoje o mais bem sucedido ataque cibernético que se tem conhecimento. Tornou-se uma referência e a tendência é que os ataques tornem-se cada vez mais complexos e difíceis de se identificar. O Stuxnet afetou milhares de computadores em usinas nucleares ao redor do mundo, mas a principal usina afetada foi a de Natanz, no Irã, o que para muitos é o suficiente para afirmar que o principal objetivo do ataque era sabotar o programa nuclear iraniano. O vírus agia discretamente, a vítima não tinha ideia de que estava sob ataque. Um novo tipo de arma tinha sido descoberto, um ataque cibernético capaz de gerar danos físicos à uma estrutura crítica. A partir desse momento houve uma maior preocupação por parte dos Estados em relação à ataques cibernéticos e como se defender (SINGER; FRIEDMAN, 2014).

O terceiro capítulo é um registro comparativo entre as políticas para a defesa cibernética dos Estados Unidos e do Brasil. Os Estados unidos são uma escolha natural para a análise. Por serem a maior potência mundial, suas ações são observadas por todo o mundo e muitas vezes servem de referência para o desenvolvimento das políticas de outros países. O Brasil foi escolhido com o intuito de comparar as principais semelhanças e diferenças entre as políticas nacionais e as americanas, além de destacar os esforços brasileiros no desenvolvimento da sua política de defesa.

1 O ESPAÇO CIBERNÉTICO NAS RELAÇÕES INTERNACIONAIS

A expansão do espaço cibernético e a popularização dos seus meios de acesso forneceram benefícios inegáveis para a população mundial, sendo uma das principais causas da compressão espaço tempo que representa a globalização. A Tecnologia da Informação e Comunicação (TIC) é um avanço tecnológico irreversível. Seja por meio de computadores, *smartphones* ou *tablets*, atualmente estamos ininterruptamente recebendo informações, compartilhando-as e fazendo parte da expansão deste espaço cibernético.

John Arquilla e David Ronfeldt (1993), em "*Cyberwar is Coming!*", deram o aviso sobre a chegada de um novo estilo de guerra, a guerra cibernética. Nas ideias de Arquilla a guerra cibernética refere-se a conduzir e preparar operações militares de acordo com princípios relacionados à informação, ou seja, tentar saber tudo sobre o adversário enquanto tenta evitar que o adversário obtenha informações sobre você, usar mais conhecimento para usar menos capital e trabalho (ARQUILLA; RONFELDT, 1993). Outras visões sobre o conceito de guerra cibernética serão apresentados mais adiante.

Diferente de ataques militares convencionais, os ataques cibernéticos não ocorrem apenas entre instituições e alvos militares. Ataques cibernéticos, em algum momento visam alvos militares, mas não exclusivamente. O conflito cibernético também vai ter como alvo companhias de grande importância para os indivíduos e a infraestrutura dos Estados. Empresas privadas estão suscetíveis a sofrerem ataques como forma de atingir um estado ou a ideologia que aquela empresa representa (BRENNER, 2010).

No ano de 2007 e de 2008, diversos sites da Estônia e da Geórgia, respectivamente, ambos os casos em conflito contra a Rússia, sofreram ataques do tipo Distribuídos por Negação de Serviço (DDoS). Este tipo de ataque ocorre quando servidores são sobrecarregados por causa de numerosos acessos simultâneos originados de diversos computadores *zumbis*, computadores que são controlados remotamente para causar uma inundação de acessos. Esta sobrecarga faz com que os

servidores parem de responder e assim os sites ficam fora do ar por um tempo indeterminado (GRAÇA, 2013).

Em 2007 Rússia e Estônia passavam por um momento de tensão devido à mudança de local da estátua Soldado de bronze de Tallinn, estátua que marcava a vitória russa contra o nazismo na segunda guerra mundial. A partir da mudança de local da estátua a Estônia passou a ser alvo de vários ataques cibernéticos. Na época, este seria o primeiro ataque cibernético de Estado contra outro Estado (TRAYNOR, 2007), porém o envolvimento do governo russo nunca foi confirmado (SPUTNIKNEWS, 2007).

No verão de 2008 as tensões entre os separatistas da Ossétia do Sul, região apoiada pelos russos, e a Geórgia elevaram-se ao ponto de desencadear um conflito armado internacional (KING, 2008). Porém, o que se observou antes dos ataques armados foi um ataque DDoS a diversos servidores do governo da Georgia. Sites como a página oficial do presidente georgiano Mikheil Saakashvili, o site central do governo, a página do Ministério das Relações Exteriores e do Ministério da Defesa, ficaram fora do ar (SWAINE, 2008).

Caso semelhante aconteceu durante a crise da Crimeia em 2014, quando diversos sites da Organização Tratado do Atlântico Norte (OTAN) sofreram ataques DDoS (LOBATO; KENKEL, 2015). A crise da Crimeia foi uma consequência da revolução ucraniana de 2014. Após o governo de Viktor Yanukovych ter sido deposto na Ucrânia grande parte da população da Crimeia, predominantemente russófona, mostrou-se descontente com os rumos contrários à Rússia que o novo governo tomava. Em 16 de março de 2014, as autoridades pró-Rússia da Crimeia propuseram um referendo interno perguntando aos habitantes se estes gostariam de ser anexados pela Rússia, o resultado foi positivo com grande vantagem. Durante o a escalada das tenções diversos sites públicos da OTAN foram alvos de ataques DDoS (CROFT; APPS, 2014).

Dos acontecimentos recentes de ataques cibernéticos, o que mais chamou a atenção nos últimos anos foi o a descoberta do vírus Stuxnet em 2010, o primeiro ataque cibernético registrado contra uma infraestrutura industrial (LOBATO; KENKEL, 2015). No caso Stuxnet, o sistema digital de controle de centrífugas nucleares de uma

usina iraniana foi infectado por um vírus que parou parte das centrífugas. O que pode ter impedido o país de gerar energia nuclear (CEPIK; CANABARRO; BORNE, 2014). O Stuxnet se destacou como uma nova arma, já que foi planejado para causar danos físicos por meio de uma rede cibernética. Esses danos físicos foram consideráveis, mas eficientes e não causaram nenhuma morte. Muito diferente de ataques militares por meios convencionais (SINGER; FRIEDMAN, 2014).

Cavelty (2012) afirma que o caso do Stuxnet é a manifestação de um temor de longa data. Foi um ataque invisível e impossível de rastrear, que afetou o sistema de controle de uma infraestrutura crítica. Talvez o maior efeito que o Stuxnet tenha causado é o fator medo. Ele deixou diversos oficiais de Estado aterrorizados. Em nível nacional governos começaram a lançar e atualizar estratégias de segurança cibernética. E em nível internacional uma atenção crescente tem sido dada para o aspecto estratégico e militar do espaço cibernético.

Fazendo um breve apanhado dos casos de ataques cibernéticos que ocorreram por motivações políticas os Estados tendem a não assumir suas responsabilidades e negam qualquer envolvimento, como fizeram os russos no caso da Estônia em 2007 e da Geórgia em 2008, assim como os americanos e israelenses no famoso episódio do Stuxnet em 2010. Essa omissão de responsabilidade é favorecida pelo anonimato do espaço cibernético e pela dificuldade de se colher provas e evidências da ligação entre um Estado e um ataque cibernético (JENSEN, 2014).

Esses ataques não são exclusivos de tempos de guerra e ocorrem a todo instante. Somente no ano de 2008, os ataques dirigidos aos sites do governo americano ".gov" ou ".mil" chegaram na casa dos milhares e companhias tiveram um prejuízo médio de 2 milhões de doláres no ano de 2009 por causa de ataques cibernéticos (DEMCHAK; DOMBROWSKI, 2011). O reconhecimento do espaço cibernético como um novo campo de ação nas Relações Internacionais está resultando em um processo de securitização do espaço cibernético (LOBATO; KENKEL, 2015).

Como disse Duarte (2012) , a preparação da defesa nacional de um Estado é uma necessidade que faz parte da condição anárquica do sistema internacional e novas tecnologias fazem parte desta reflexão ainda mais quando causam uma competição por

superioridade militar entre os atores. O espaço cibernético possui características únicas nas relações entre os atores do sistema internacional. Não há uma divisão clara entre as causas e consequências no espaço virtual e no mundo físico, o espaço cibernético permite agir de modo anônimo e tudo isso pode ser acessado por meio de equipamentos de baixo custo disponíveis para a população em geral (LOBATO; KENKEL, 2015). Essa característica anônima do espaço cibernético favorece os responsáveis pelos ataques, seja um indivíduo ou um Estado, impossibilitando uma retaliação.

Para entender melhor a importância e o poder do espaço cibernético nas Relações Internacionais podemos utilizar como exemplo os vazamentos do caso Snowden. Os documentos vazados pelo ex-técnico da CIA e consultor da Agência de Segurança Nacional (NSA) revelam que os EUA estavam espionando líderes mundiais em nome da “segurança nacional”. Os documentos ainda revelam que governos não eram os únicos alvos mas também empresas multinacionais, como a Petrobras, derrubando a alegação de que os grampos tinham como interesse a segurança americana (KAZ, 2013).

Nazli Choucri (2013) listou os dez maiores impactos que as Relações Internacionais sofreram com a evolução do espaço cibernético.

> Primeiro: O empoderamento de novos atores. Entre eles entidades nacionais, entidades comerciais não estatais com novos produtos e processos, agentes agindo em nome de atores estatais, novos grupos criminosos variados e anônimos e a emergência de novos mercados não-regulados.
>
> Segundo: Uma mudança na tradicional relação de poder e a criação de novas oportunidades para atores mais fracos ameaçarem os mais poderosos, para uso variado do anonimato, para novos ramos de atividade política, industrial ou militar e para a expansão de atividades criminosas.
>
> Terceiro: Novos desafios para a segurança nacional, de fontes de vulnerabilidade sem precedentes, novas dimensões de segurança nacional combinadas com incerteza, medo e ameaças de fontes desconhecidas.
>
> Quarto: Diversas formas de conflito cibernético e contenções criam novos desafios para a estabilidade e segurança do sistema estatal, como a militarização do espaço cibernético, a conduta da guerra cibernética, ameaças às infraestruturas críticas, espionagem cibernética, etc.
>
> Quinto: Crescimento e poder sem precedentes de instituições para gerenciamento do espaço cibernético, ou para ajudar a apoiar a segurança cibernética.

> Sexto: Uma significativa desconfiança por parte de tradicionais instituições internacionais que questionam a legitimidade das novas instituições para gerenciamento do espaço cibernético.
>
> Sétimo: O aumento de tomadores de decisões para domínio cibernético com mandatos incertos e descrições de trabalho sobrepostas criam ambiguidades que escondem responsabilidades, questiona a legitimidade e aumenta a incerteza.
>
> Oitavo: Nova demanda por cooperação cibernética para conter o crescimento de conflitos cibernéticos mais tarde reforçado por um crescente empurrão para definir as normas cibernéticas globais.
>
> Nono: A nova atrelagem de política nos meios cibernético e tradicional moldam novas estratégias baseadas para alavancar o domínio cruzado e negociações que raramente são consistentes com a prática convencional.
>
> Décimo: O efeito transformativo do acesso cibernético permeia todos os níveis de análise nas Relações Internacionais - os indivíduos, o Estado, o sistema internacional e o sistema global - incluindo atores transnacionais e não estatais, por lucro ou não (CHOUCRI, 2013, p.8, tradução nossa).

Em 2012, a mesma Nazli Choucri, em parceria com Robert Reardon, ambos do departamento de ciências políticas do Massachusetts Institute of Technology (MIT), prepararam uma revisão da literatura na língua inglesa da primeira década do século XXI, 2001 - 2010, com o tema de espaço cibernético. Reardon e Choucri analisaram 49 artigos (de 49 autores) escritos em inglês de diversas revistas científicas das áreas de Ciências Políticas e Relações Internacionais. Em sua maioria estes artigos acabam se encaixando em uma de cinco áreas distintas: sociedade civil global, governança, desenvolvimento econômico, os efeitos em regimes autoritários e segurança (REARDON; CHOUCRI, 2012).

Reardon e Choucri (2012) em seu levantamento literário, perceberam que a maioria dos artigos acadêmicos sobre o espaço cibernético são baseados na teoria construtivista. O senso comum das Relações Internacionais aponta o realismo como teoria principal quando o assunto é segurança nacional mas as pesquisas mais recentes fazem a análise do espaço cibernético por meio da teoria construtivista e a securitização do tema.

Dando continuidade a seu artigo, Reardon e Choucri (2012) apresentam uma imagem um pouco mais detalhada dos cinco temas recorrentes quando o assunto é espaço cibernético. Começando por espaço cibernético e uma sociedade civil global, os autores lembram que nas últimas décadas houve um movimento sugerindo que a popularização dos meios de comunicação criariam uma sociedade civil global.

Todos os autores analisados por Reardon e Choucri (2012) veem o espaço cibernético como um mecanismo de empoderamento. Em contrapartida alguns dos autores que tinham em mente a ideia de uma sociedade civil global serão limitados pelo fato de as relações via espaço cibernético serem mais fracas do que as relações interpessoais e que os usuários dos espaço cibernético muitas vezes estão mais preocupados com entretenimento do que com discussões políticas e sociais.

Um dos assuntos mais comentados sobre o espaço cibernético é a questão da governança. Há um debate sobre padrões técnicos, regulações e quais instituições determinariam a estrutura do espaço cibernético. Todos os textos analisados sobre o assunto levantam a preocupação de qual seria o papel do Estado neste processo (REARDON; CHOUCRI, 2012).

O desenvolvimento econômico é uma área que tradicionalmente tem sido tratada com muito otimismo, principalmente no aspecto do crescimento econômico por meio da velocidade da informação no espaço cibernético. Essa visão encontra uma barreira no mundo real. Muitos países com população pobre não têm acesso a essa rede de conhecimento e em lugares com uma alta desigualdade social esse desequilíbrio de acesso pode causar revoltas por partes das populações menos favorecidas (REARDON; CHOUCRI, 2012).

O espaço cibernético coloca os regimes autoritários em um dilema. As vantagens da rede são inegáveis, incluindo os benefícios econômicos. Mas o espaço livre para o debate coloca os regimes autoritários em perigo. Há um sistema complexo de controle que pode ser usado por regimes autoritários em seu favor, como faz, por exemplo, a China. A rede chinesa é altamente censurada e ampara atividades de apoio ao governo em o que o autor chama de um sistema semi-permeável, em que o Estado não pode controlar a grande quantidade de *websites* que podem ser acessados mas pode levantar barreiras quando o assunto é páginas com conteúdo sensível para o governo. O espaço cibernético chinês possui redes sociais semelhantes e baseadas nos mesmo modelos das ocidentais, porém são utilizadas quase que exclusivamente por usuários chineses, o que acaba criando uma exclusão dos assuntos populares nas redes ocidentais, criando um ambiente focado nos acontecimentos chineses. Mas nem

todos os regimes autoritários utilizam esse mesmo sistema. A Coréia do Norte por exemplo, que escolheu não promover o acesso ao espaço cibernético, isolando-se também no mundo cibernético (REARDON; CHOUCRI, 2012).

Dos 49 artigos examinados por Reardon, 19 eram focados na segurança no espaço cibernético. Este por sua vez será o assunto principal analisado por esta pesquisa. Nesta área foi discutida uma grande variedade de assuntos, o que levantou a dúvida de Reardon sobre qual seria o significado exato quando os autores se referem a “conflito cibernético”, "segurança cibernética" ou "guerra cibernética". As temáticas abordadas nos assuntos vão desde propaganda, informação operacional, ataques estratégicos e espionagem. Há dois diferentes níveis de debate nesta literatura. Em um há o debate sobre a natureza da ameaça e os meios de concretizá-la, em outro há um debate sobre a ontologia e a epistemologia da segurança cibernética e a evolução do conceito, este trabalho se aproximará do primeiro debate. (REARDON; CHOUCRI, 2012).

Parte dos autores analisados por Reardon consideram a tecnologia da informação como uma tecnologia militar que veio para aprimorar as tradicionais formas de combate. Goldman (2004) descreveu a tecnologia da informação como um intensificador da eficiência que permite militares distribuírem grandes quantidades de informação e identificar o que é útil estrategicamente. A tecnologia seria útil para Estados que já possuem capacidades militares sofisticadas. Por outro lado, Newmyer (2010) vê a tecnologia da informação como uma ferramenta capaz de interromper os sistemas de informação dos adversários.

Outra parte foca mais na importância de formas cibernéticas de organizações militares, como por exemplo a capacidade de unidades móveis adaptarem suas estratégias baseadas em informações recebidas em tempo real (BOUSQUET, 2008). Luttwak (2002) tem uma visão semelhante e argumenta que os estrategistas das forças americanas têm uma visão falha em considerar a tecnologia da informação como uma mera tecnologia para aumento de capacidade, quando na verdade ela requer uma transformação qualitativa para ser totalmente aproveitada.

Há também autores que descrevem o espaço cibernético como um novo domínio de conflito, mas há um desacordo sobre a natureza da ameaça. Uma vez que, analisando os crescentes ataques cibernéticos, é possível observar que grande parte dos “ataques” são casos de espionagem, o que não caracteriza um ataque segundo as leis internacionais de guerra, mas somente uma nova ferramenta dentro da guerra tradicional (CLARKE, 2009).

Existe um consenso de que estratégia de ataques contra estruturas críticas são uma grande ameaça para a segurança nacional. Essa estratégia pode ser vantajosa para um adversário, uma vez que é algo barato de se realizar e ao mesmo tempo é difícil fazer a ligação com confiança do ataque a um ator em especial. Esses ataques são particularmente interessantes uma vez que o custo para realizá-los é consideravelmente baixo, ao mesmo tempo em que uma defesa cibernética tem um custo elevado, mas essas visões fazem parte da literatura política, que possui um caráter mais realista (REARDON; CHOUCRI, 2012).

Na literatura acadêmica, o espaço cibernético é frequentemente analisado com uma visão mais construtivista. A literatura construtivista, em particular a securitização, tem em foco temáticas que antes não eram vistas como questões de segurança mas que passam a ser tratadas como tal. Outro foco da visão construtivista sobre o espaço cibernético é como o a segurança cibernética tem sido interpretada como uma ameaça à segurança nacional. Nesta análise se destaca Lene Hansen e Helen Nissenbaum (REARDON; CHOUCRI, 2012).

Para Dartnell (2003) a ameaça do espaço cibernético não é os Estados agindo taticamente, mas sim os atores não estatais que espalham internacionalmente suas ideias radicais de maneira estratégica, assim como para Der Derian (2003) o foco está nas ideias, que não são uma ameaça física, mas podem desestabilizar as ordens políticas e sociais. Há uma preocupação com o uso do espaço cibernético por terroristas para organizar, recrutar e coordenar ataques. De acordo com Clarke e Porche III (2016), o grupo terrorista Estado Islâmico tem usado o espaço cibernético como ferramenta de propaganda e recrutamento.

O anonimato da rede permite a grupos terroristas agirem sem serem rastreados, de tal forma que vários grupos terroristas possuem *websites* oficiais. Outro fenômeno que é possibilitado graças ao anonimato da rede é a ligação de organizações, terroristas ou não, com Estados, uma vez que estes dispõem de mais recursos e capacidades, e assim se escondem por trás destas organizações. Por outro lado este mesmo anonimato que protege a identidade de grupos terroristas pode ser frustrante para eles, uma vez que os grupos terroristas agem com a intenção de ganhar atenção e notoriedade, eles tem como objetivo a realização de atos aos quais a autoria pode ser aclamada. Há, ainda, a possibilidade de grupos terroristas usarem a rede para criar uma campanha de "cyber medo", divulgando uma visão exagerada das suas reais capacidades e assim causando uma reação de medo real na população (CEPIK; CANABARRO; BORNE, 2014).

Hansen e Nissembaum (2009) analisam o tema segurança cibernética de acordo com a visão da Escola de Copenhagen e o conceito de securitização. Segundo Lobato e Kenkel (2015), a securitização do espaço cibernético não está livre de controvérsias e não ocorre em países que são menos dependentes dos sistemas de informação. Há, ainda, por parte dos EUA a transição da securitização para a militarização do espaço cibernético, uma vez que o discurso de securitização teve início nesta super potência e outras potências tendem a seguir seus discursos (LOBATO; KENKEL, 2015).

A academia brasileira tem lançado trabalhos em consonância com os artigos publicados nas revistas internacionais. Luiza Cruz Lobato e Kai Michael Kenkel (2015) da PUC-RJ publicaram seu artigo *Discourses of cyberspace securitization in Brazil and in the United States* que faz uma comparação entre os discursos de securitização da Escola de Copenhague no Brasil e nos Estados Unidos.

A Escola de Copenhague busca uma nova visão para Sistema Internacional pós-Guerra Fria, ampliando e redefinindo as questões de importância na área de Segurança Internacional (ACÁCIO, 2011). O conceito de securitização da Escola de Copenhague foi desenvolvido por Buzan, Waever e Wilde (1998) e diz que quando um

assunto passa a ser legitimamente percebido como ameaça é o suficiente para a adoção de medidas que garantam a segurança (CEPIK; CANABARRO; BORNE, 2014).

> Securitização é um conceito desenvolvido por Buzan, Wæver e Wilde (1998), da Escola de Copenhague. Para os autores, que procuram sintetizar correntes realistas e construtivistas da Teoria das Relações Internacionais, o estudo da segurança e/ou da insegurança deve englobar tanto aspectos materiais – armas, distribuição de poder, questões demográficas etc. – quanto imateriais próprios das fontes de insegurança. Os aspectos imateriais se referem a processos sociocognitivos de interpretação de ameaças inerentes à forma com a qual determinado assunto – não necessariamente relacionado ao emprego da força, como, por exemplo, o caso das migrações ou a degradação do meio ambiente – é enquadrado como ameaça existencial a um objeto de referência – a população do país que recebe migrantes, ou a humanidade, respectivamente, no caso dos exemplos citados anteriormente. Segundo a teoria, quando determinado assunto é legitimamente percebido como ameaça existencial, justifica-se a adoção de medidas extraordinárias que extrapolam a ordem regular do processo de decisão política daquele país, diante da urgência de medidas que garantam a segurança do objeto ameaçado. Inicialmente, a Escola de Copenhague identificou processos de securitização nos setores militar, econômico, ambiental, político e social das relações internacionais. Um panorama a respeito da Escola de Copenhague pode ser encontrado em Duque (2009). Mais recentemente, Hansen e Nissenbaum (2009) se propuseram a ampliar o ferramental teórico dos estudos de segurança da Escola de Copenhague, a partir da avaliação de eventos de securitização relacionados ao espaço cibernético e à Internet, agregando assim o setor cibernético à análise (CEPIK; CANABARRO; BORNE, 2014, p. 2).

Segundo Lobato e Kenkel (2015), o tema não é novidade para os americanos, que desde o início dos anos 90 já tratam o assunto como securitização. Já o lado brasileiro está um pouco mais atrasado, apenas em 2008 o espaço cibernético foi caracterizado como setor estratégico na Estratégia de Defesa Nacional (BRASIL, 2008). Em 2012 o Ministério da Defesa lançou a Política Cibernética de Defesa (BRASIL, 2012). O artigo ainda aponta que, no Brasil, o assunto é institucionalizado e que o processo de securitização ainda falta receber uma maior notoriedade e reconhecimento de agentes públicos e privados. Já nos EUA o processo é consolidado e faz parte do processo governamental, o que justifica mecanismos de vigilância e controle estatal.

Marco Cepik, Diego Rafael Canabarro e Thiago Borne da Universidade Federal do Rio Grande do Sul (UFRGS) publicaram, em 2014, o artigo A Securitização Do Espaço cibernético E O Terrorismo: Uma Abordagem Crítica, que faz uma análise geral sobre o terrorismo cibernético. Comentam sobre o início e a propagação do uso do termo em jornais e revistas americanas e apontam que nos últimos anos houve um

esforço por parte dos Estados no que se refere a preparação para uma guerra cibernética. O anonimato ainda permite a possibilidade de vinculação entre organizações criminosas e Estados, uma vez que Estados possuem mais recursos que grupos não estatais. E concluem com a afirmação de que para um ato de violência cometido através do espaço cibernético ser considerado um ato de guerra, ou terrorismo, este terá que causar danos físicos direta ou indiretamente já que ainda não existe uma desvinculação completa da Internet com o mundo terreno.

Em todo este debate de espaço cibernético e segurança cibernética, há um problema em unificar o que seria a matéria de análise. Espaço cibernético está ligado aos termos Internet, tecnologia da informação, tecnologia da comunicação e rede, mas é difícil definir qual é o termo mais apropriado para análise (REARTON; CHOUCRI, 2012).

Segundo Paulo Sergio Melo de Carvalho (2011), General da Brigada do Exército Brasileiro, o espaço cibernético é um espaço virtual formado por dispositivos computacionais que podem estar, ou não, conectados em rede. É o campo aonde as informações digitais transitam, são processadas e armazenadas. De acordo com Cepik (2014), o espaço cibernético é marcado pelo uso da eletroeletrônica e do espectro eletromagnético que tem o objetivo de criar, armazenar, modificar e trocar informações entre redes interconectadas. Segundo esta definição, as redes de telégrafo, rádio amador, telefonia fixa e móvel e a televisão por satélite já configuravam o espaço cibernético antes da criação da internet (CEPIK; CANABARRO; BORNE, 2014).

Para Carvalho (2011), a segurança cibernética, ou segurança cibernética, é definida pela proteção de dados estratégicos, principalmente aqueles que controlam as infraestruturas críticas nacionais abrangendo interações de órgãos públicos e privados.

Cavelty (2012) realizou uma tentativa de separar o conflito cibernético em seis categorias diferentes de acordo com o alvo, a origem, a intensidade e a finalidade dos ataques. Os resultados da separação realizada por Calvety são guerra cibernética, terrorismo cibernético, sabotagem cibernética, espionagem cibernética, crime cibernético e Hacktivismo.

A guerra cibernética seria o uso de computadores para prejudicar atividades de um país inimigo, como, por exemplo, ataques ao sistema de comunicação. O termo também é equivocadamente usado para definir acidentes cibernéticos de natureza política (CAVELTY, 2012).

O terrorismo cibernético são ataques contra computadores, redes e as informações armazenadas nestes, para intimidar ou coagir um governo ou sua população em nome de um objetivo político ou social.O ataque tem que resultar em violência contra pessoa ou propriedade, ou ao menos causar dano o suficiente para gerar um nível de medo para ser considerado “terrorismo cibernético”.O termo também é usado de forma equivocada para definir acidentes cibernéticos de natureza política (CAVELTY, 2012).

Sabotagem cibernética se refere ao ato de criar, por meio cibernético, a perturbação de processos militares ou econômicos para alcançar um objetivo pessoal, geralmente político. Espionagem cibernética é o acesso não autorizado com a intenção de testar as configurações ou a defesa de um computador ou a visualização e cópia de arquivos e dados. Já o crime cibernético é uma atividade criminal feita usando computadores e a Internet. E o por fim o hacktivismo é a combinação de *hacker* e ativismo, incluindo atividades que usam técnicas de *hacker* contra alvos como *websites* com a intenção de atrapalhar as atividades padrões (CAVELTY, 2012).

Espera-se que a natureza do espaço cibernético evolua e sofra uma mutação. As forças da inovação tendem para uma rápida mutação. Entretanto plataformas bem-sucedidas acumulam uma quantidade de usuários que dependem dela e essa dependência se torna um limitador da frequência de inovações (CLARKE, 2009).

Com base nas ideias dos principais autores sobre segurança cibernética, este trabalho fará uma análise da visão Construtivistas na questão da segurança no espaço cibernético. Serão utilizados trabalhos de autores como James Der Derian, Michael Dartnell e os maiores expoentes da Escola de Copenhague no âmbito do espaço cibernético, Lene Hansen e Helen Nissenbaum serão usados como base para o

debate. A análise da literatura sobre o espaço cibernético nas Relações Internacionais feita por Robert Reardon e Nazli Choucri também será uma norteadora deste estudo.

O caso recente mais emblemático envolvendo o Brasil em questões de segurança cibernética foi a espionagem americana em 2013 a diversos alvos brasileiros, desde líderes do governo, como a ex-presidente Dilma Rousseff, a empresas de exploração de petróleo, como a Petrobras, casos que trazem holofotes para a questão da segurança cibernética nacional e a crescente securitização. A atuação brasileira será analisada com base em documentos oficiais do governo e do exército brasileiro e também em trabalhos de autores como Luiza Cruz Lobato, Kai Michael Kenkel, Gustavo Diniz, Robert Muggah, Misha Glenny e Paulo Sergio Melo de Carvalho.

2 ANÁLISE HISTÓRICA

Os ataques que utilizam o cibernético como meio de realização não são exclusividade do século XXI. Há relatos de ciberataques que datam da década de 80, porém estes ataques primitivos não tinham a capacidade, a complexidade e o peso no sistema internacional que possuem os ataques modernos (RUSSELL, 2004). Nesta parte da pesquisa, será feita uma análise histórica dos principais acontecimentos internacionais envolvendo Estados e o espaço cibernético. Serão analisados os casos de ataques DDoS contra a Estônia em 2007 e contra a Geórgia em 2008 e o Stuxnet em 2009, caso mais emblemático de ataque internacional cibernético.

2.1 Estônia

Em 2007 a Estônia era considerada um dos países mais conectados da Europa. Em 1997 97% das escolas estonianas estavam online. Em 2000, as reuniões de gabinete do governo passaram a não usar papéis. Em 2002, a maioria da zona habitada estava coberta por uma rede sem fio gratuita fornecida pelo governo. Em 2007, foi introduzida a votação online e 90% das transações de banco já eram feitas pela internet (HAMMERSLEY, 2015).Com toda essa conectividade, um ataque cibernético à rede estoniana seria capaz de parar boa parte do país. E foi isso o que aconteceu em 27 de abril de 2007.

Nessa data, o governo estoniano decidiu mudar de lugar uma estátua soviética de 1947 que ficava no centro de Tallinn, capital da Estônia. Para muitos cidadãos estonianos a estátua representava a opressão da ocupação soviética e após 16 anos da independência, eles removeriam a estátua do centro da capital, mesmo com protestos e avisos do governo russo, que avisara que a remoção da estátua seria "desastrosa para os estonianos". Alguns dias depois, a estátua foi instalada em um cemitério militar nos arredores da cidade (WIRED, 2007).

Mesmo antes da remoção da estátua, protestos já estavam ocorrendo em Tallinn. Ocorreram depredações de propriedades comerciais e privadas e confrontos com a polícia. A maioria dos que iam para a rua protestar eram cidadãos de etnia russa

contrários à remoção do monumento soviétivo. Os protestos duraram uma noite e parecia que a situação se acalmaria (WIRED, 2007).

No dia 26 de abril, junto com os protestos de rua, havia começado um ataque DDoS, um ataque que sobrecarrega servidores, contra o governo estoniano. O ataque passou despercebido nas primeiras 24 horas e só foi descoberto quando o ministro da defesa estoniano, Jaak Aaviksoo, não conseguiu efetuar o *login* no site de seu partido. O ataque começou no site do partido e depois se espalhou para outros partidos e sites do governo. No final de uma semana, os ataques DDoS deixariam estes sites completamente fora do ar (RICHARDS, 2009).

Na semana seguinte os ataques continuaram e agora afetavam os sites das principais redes de notícias estonianas. Os milhares de acessos que derrubaram os sites foram rastreados e tinham origem de fora do país. A única maneira que os sites de notícias encontraram para voltar ao ar foi negando qualquer acesso internacional às páginas (RICHARDS, 2009).

Os ataques continuaram por mais duas semanas quando, em 9 de maio, à meia-noite do horário de Moscou, a Estônia sofreu o maior ataque até então. Neste ataque, o alvo foi o sistema bancário que sofreu mais de 4 milhões de acessos por segundo. Para se proteger dos ataques, o Hansabank, maior banco da Estônia, teve que desligar suas operações onlines. O desligamento teve três consequências principais. A primeira foi a interrupção das transações onlines, que representavam mais de 90% das transações bancárias do país. A segunda foi a interrupção das comunicações entre o banco e os seus caixas eletrônicos. E por último a paralisação da comunicação com os outros sistemas bancários do mundo, o que interrompeu as transações com cartões de débito de correntistas ao redor do mundo e isolou o sistema bancário estoniano (RICHARDS, 2009).

Após os ataques, o governo estoniano acusou o governo russo de ser o responsável pelos ataques, que negou todas as acusações de envolvimento. Até os dias atuais não se sabe qual foi o envolvimento do governo russo nos ataques. O que se sabe é que os hackers atacaram por sua própria iniciativa, primeiramente como forma de protesto político. Esses hacktivistas eram tanto hackers experientes, que

escreviam seus próprios códigos maliciosos, quanto novatos, que seguiam guias passo-a-passo de como atacar os alvos. O governo estoniano prendeu apenas uma pessoa, um estudante de etnia russa, que morava na Estônia (RICHARDS, 2009).

A prisão de uma pessoa não foi o único efeito colateral dos ataques. O governo da Estônia e a OTAN lançaram ações de conscientização das vulnerabilidades cibernéticas. A OTAN abriu um centro de defesa cibernética em Tallinn, o CCDCOE ou Centro de Excelência Cibernética Cooperativa, para estabelecer protocolos de reação à ameaças cibernéticas (RICHARDS, 2009). No ano de 2013 este centro lançou o Manual Tallinn, sobre a aplicabilidade da lei internacional na resolução de conflitos cibernéticos (NATO, 2013).

2.2 Geórgia

No ano de 2008 a Rússia foi novamente protagonista em uma caso de conflito cibernético. Neste caso, o alvo foi a Geórgia. A Ossétia do Sul é uma região separatista da Geórgia localizada ao norte do país. Nos anos 90 houve uma guerra civil e desde então a região vem buscando reconhecimento da sua independência da Geórgia, com apoio do governo russo. O povo da Ossétia do Sul tem cultura e idiomas diferentes do georgianos e buscavam se juntar à Ossétia do Norte, uma federação autônoma dentro da Rússia (BBC BRASIL, 2008).

Em abril de 2008, a OTAN acenou para a Geórgia com a possibilidade de no futuro esta vir a se juntar à aliança militar, o que causou uma forte reação russa, que é contrária à expansão da OTAN para perto de suas fronteiras. Com essa insatisfação, a Rússia permitiu que aviões militares sobrevoassem a região da Ossétia do Sul, o que escalou para um confronto entre forças da Geórgia e os separatistas, apoiados pela Rússia, que já se enfrentavam em confrontos esporádicos desde os anos 90 (BBC BRASIL, 2008).

Semanas antes de os ataques em solo começarem, diversos servidores de computadores da Geórgia vinham sofrendo ataques DDoS, incluindo o site do presidente, Mikheil Saakashvili, que ficou fora do ar por 24 horas. Sites de mídias, comunicação, companhias de transporte e bancos também foram alvos de ataques

.Assim como no caso da Estônia, não se sabe ao certo quem estava por trás dos ataques. O governo da Geórgia acusou o governo russo, que por sua vez afirma não estar envolvido. Na época em que os ataques ocorreram, a Geórgia não era um país tão conectado quanto a Estônia. Por isso os impactos destes ciberataques foram bem menos impactantes para a população e o governo da Geórgia (MARKOFF, 2008).

2.3 Stuxnet

Em junho de 2010 foi descoberto o uso da primeira, e até hoje a mais simbólica, arma cibernética de cunho militar, o Stuxnet. O Stuxnet é um *worm* criado para infectar sistemas responsáveis pelo controle de equipamentos industriais (G1, 2010). O *worm* ficou mais conhecido por ter infectado e diminuído a capacidade de enriquecimento de urânio de instalações nucleares do Irã. Porém o Stuxnet também infectou milhares de outros computadores em usinas nucleares ao redor do mundo, o que levantou uma preocupação sobre a capacidade de proliferação descontrolada de um ataque cibernético por meio de vírus (FARWELL; ROHOZINSKI, 2011).

Diferente do que acontecia até então nos casos de ataques cibernéticos, o Stuxnet não tinha como objetivo a espionagem cibernética ou o congestionamento de servidores. Ele não roubava, não manipulava e nem apagava informações. Seu objetivo era destruir, fisicamente, o equipamento infectado (LANGNER, 2011). O Stuxnet era diferente de tudo que se conhecia até o momento. À época, a revista digital *Computer World* caracterizou o Stuxnet como *"one of the most sophisticated and unusual pieces of software ever created"*, em tradução livre "um dos mais sofisticados e incomuns exemplos de *softwares* já criados" (FARWELL; ROHOZINSKI, 2011).

Um *software* tão inovador e complexo exigiria um montante considerável de investimentos, o que leva a crer que o Stuxnet foi financiado por algum grupo com muitos recursos e grandes interesses. Por este motivo o envolvimento de um Estado é praticamente dado como certo, porém até hoje é desconhecida a origem do vírus. Segundo Farwell e Rohozinski o que mais chama a atenção é a confluência entre o crime cibernético e a ação de Estados. Estados estão capitalizando tecnologias que são desenvolvidas por organizações especializadas em crimes cibernéticos e muito

provavelmente estão terceirizando ataques cibernéticos à partes que não podem ser responsabilizadas ou rastreadas, incluindo organizações criminosas (FARWELL; ROHOZINSKI, 2011).

Pode-se observar pelo código de programação que os programadores do *worm* fizeram o máximo para limitar a propagação do Stuxnet. Eles não escolheram os meio de propagação convencional de um *worm*, ele só poderia ser transmitido via USB, por *pen drives* ou por redes locais. E mesmo podendo infectar qualquer computador rodando um sistema operacional Windows, ele só entrava em ação quando encontrava um controlador de sistemas industriais da marca alemã Siemens, a mesma usada nas instalações iranianas da cidade de Natanzs e ficava inativo até o momento em que todas as centrífugas estivessem completamente carregadas e em atividade. Quando o Stuxnet entrava em atividade, a frequência de rotação das centrífugas era aumentada, causando a destruição do equipamento (LANGNER, 2011).

Mesmo com toda a precaução para que o Stuxnet não se espalhasse, o vírus atingiu aproximadamente 100.000 computadores em todo o mundo mas só entrou em atividade na usina de Natanzs. O que gera muito peso à teoria de que o vírus foi desenvolvido para atuar naquela usina especificamente (LANGNER, 2011). O Stuxnet atuou nas centrífugas da usina. Esta etapa do enriquecimento de urânio usa uma alta velocidade para separar os isótopos de urânio-235 para serem usados em reatores de energia ou até mesmo como material de fissão para armas nucleares (FARWELL; ROHOZINSKI, 2011).

O Stuxnet agia alternando a frequência da corrente elétrica que alimentava as centrífugas, o que, consequentemente, gerava uma alternância de velocidade para qual as máquinas não foram programadas. Isto ocorreu durante meses. Essa variação de velocidade era a responsável por criar a deficiência no processo de enriquecimento de urânio que sabotava as operações normais da usina (FARWELL; ROHOZINSKI, 2011).

Ainda é incerto o quão efetivo o ataque com o Stuxnet foi. O ministro das comunicações do Irã, Reza Taghipour, afirmou que o efeito do vírus nos sistemas governamentais não foi sério e que todos os locais infectados foram identificados e

resolvidos (FARWELL; ROHOZINSKI, 2011). Ahmadinejad chegou a admitir que o Stuxnet atrasou o programa nuclear iraniano, mas que o vírus atacou um número limitado de centrífugas (FARWELL; ROHOZINSKI, 2011). Inspetores da agência atômica internacional afirmaram que, durante uma semana no mês de novembro de 2009, o Irã cessou o abastecimento de urânio nas centrífugas de Natanz e que entre o meio de 2009 e 2010 houve um decréscimo de 23% no número de centrífugas operantes, resultados que podem ser ligados à ação do Stuxnet (FARWELL; ROHOZINSKI, 2011).

O que causou mais preocupação com o Stuxnet foi a nova fronteira que os ataques cibernéticos estavam alcançando, a fronteira de danos físicos à infraestruturas vitais. Após um ataque à usinas nucleares fica a preocupação com outras estruturas, como outras usinas de energia, hidrelétricas e termelétricas, sistemas de trânsito e o controle do tráfego aéreo. Esta nova modalidade de ataques pode nos levar a um futuro com vírus cada vez mais sofisticados e que causam danos cada vez maiores, incluindo vidas humanas (FARWELL; ROHOZINSKI, 2011).

Um dos principais pontos de debate em relação à segurança cibernética é a normatização do espaço cibernético. A resolução 3314 da Assembleia Geral da ONU define agressão como "[...] o uso da força armada por um Estado contra a soberania, integridade territorial ou independência política de outro Estado, ou de qualquer forma incompatível com a Carta das Nações Unidas, tal Como decorre da presente Definição" (ONU, 1973, p.2). Nesta definição, um ataque cibernético não seria classificado como agressão por não se configurar um ataque armado contra a integridade territorial de um Estado. Porém a definição é anterior ao advento do conflito cibernético (FARWELL; ROHOZINSKI, 2011).

Ataques cibernéticos que causem danos físicos ou atentem contra a vida de pessoas podem ser qualificados como uso da força e um ataque armado. Em 1999, Michael Schmitt classificou ataques à redes de computadores em sete categorias, para definir se estes se caracterizavam, ou não, como uso da força (SCHMITT, 1999).

Primeiro de acordo com a severidade. Se pessoas foram mortas ou se houve uma grande destruição de propriedade, a ação provavelmente é militar. Quanto menos

dano menos provável de a ação ser qualificada como uso da força (OWENS; KENNETH; HERBERT, 2009).

Quanto à iminência, se as consequências do ataque são vistas em questão de segundos, como em uma explosão, a operação provavelmente é militar, se o efeito demora semanas ou meses para aparecer então é mais provável que seja uma ação diplomática ou econômica, comparável a um embargo (OWENS; KENNETH; HERBERT, 2009).

O terceiro ponto a se observar é a relação de causa e efeito. Se a ação é a causa único do resultado então é provável que se caracterize como uso da força. Quanto maior a ligação entre a causa e o efeito, maior a ligação com a natureza militar do ato (OWENS; KENNETH; HERBERT, 2009).

Outro ponto levantado é a invasão. Uma invasão de fronteira é um ato claro de operação militar. Ações que são realizadas de fora das fronteiras de um Estado alvo são provavelmente diplomáticas ou econômicas (OWENS; KENNETH; HERBERT, 2009).

Se o efeito de um ataque pode ser qualificado imediatamente, como escombros em chamas aonde costumava ser um edifício, a operação tem um forte caráter militar. Quanto mais subjetivo o processo para avaliar os danos causados maior a possibilidade de se tratar de uma ação econômica ou diplomática (OWENS; KENNETH; HERBERT, 2009).

A legitimidade dos ataques também pode ser determinante. O Estados possuem o monopólio do uso legítimo da força. O espaço cibernético permite que uma gama de atores realizem ataques variados. Ações que não foram de autoria de Estados tem poucas chances de serem consideradas como uma ação militar (OWENS; KENNETH; HERBERT, 2009).

E por último a responsabilidade. A partir do momento em que um Estado assume total responsabilidade de um ataque as chances de este ser caracterizado como um ato militar são maiores. Quanto maior a dúvida sobre a responsabilidade do ataque maior a chance de não ser classificado como ação militar (OWENS; KENNETH; HERBERT, 2009).

Para exemplificar o que pode ser considerado como uso da força e ataque armado via o espaço cibernético Farwell e Rohozinski citam o exemplo de uma invasão ao sistema de controle de tráfego aéreo. A partir do momento em que uma queda de avião é causada pelo queda de um sistema de controle de tráfego, seja por meio de ataque DDoS interrompendo suas funções, seja pela contaminação por meio de vírus e malware, o ato é considerado como o uso da força, não pelo meios usados mas sim pelas casualidades (FARWELL; ROHOZINSKI, 2011).

Ataques cibernéticos que venham a causar danos reparáveis, sem consequências a longo termo e sem vítimas, não serão consideradas como uso da força (FARWELL; ROHOZINSKI, 2011). Farwell e Rohozinski (2011), levantam o questionamento sobre como o mundo ocidental lidaria com um ataque que derrube toda a sua infraestrutura crítica, como o sistema financeiro, que afetaria o comércio, a economia e empregos, este ataque seria considerado como uso da força, mesmo sem vítimas fatais? Qual seria a diferença entre esses sistemas serem derrubados por via cibernética ou atacados com mísseis? A resposta apresentada pelos autores é subjetiva. Segundo Farwell e Rohozinski (2011), as respostas seriam dadas por via política, diplomática e estratégica por parte dos Estados, e não por um debate abstrato sobre regras e direito internacional.

Em 2009, foi lançado pela OTAN o Manual Tallinn sobre o Direito Internacional aplicável a guerra cibernética, um manual feito por especialistas que discorre sobre a aplicabilidade da lei internacional nos casos de conflitos cibernéticos. O Manual sugere uma definição sobre uso da força no espaço cibernético. Uma ação cibernética constitui uso da força quando seus efeitos são comparáveis à operações não cibernéticas que são caracterizadas como uso da força, como por exemplo danos estruturais e a perda de vidas humanas (AZZOPARDI, 2013). Atualmente, no ano de 2016, está em produção uma segunda versão do Manual Tallinn, o Manual Tallinn 2.0, com definições e normas internacionais mais recentes.

Utilizando essas definições como base podemos apontar, entre os casos citados, que o Stuxnet foi o ataque cibernético que mais se aproximou do uso da força. Os danos físicos causados à uma instalação de infraestrutura crítica de um Estado,

mesmo que sem vítimas, mas com um objetivo de sabotagem com indícios de que o ataque partiu de outro Estado com grandes capacidades tecnológicas e disponibilidade de recursos, levam a crer que o Irã foi vítima de um ataque estratégico de demonstração de força e superioridade tecnológica. O ataque DDoS à Estônia teve um grande impacto, tanto ao Estado, quanto aos cidadão, devido a grande conectividade do país e não à sofisticação do ataque. Ataques DDoS são relativamente simples e tem um custo baixo para o agressor, portanto não são vistos como uma grande demonstração de força estatal, mas sim como de capacidade de mobilização, já que é o tipo de ataque mais utilizado como forma de protesto por parte dos hacktivistas, os ativistas cibernéticos.

É necessário fazer uma diferenciação entre espionagem, que seria o monitoramento de dados, e a guerra cibernética. Os casos de monitoramento, como o escândalo de espionagem da NSA, ocorrem a todo instante, e chegam na casa dos bilhões de casos por ano. Os Estados utilizam o discurso de defesa nacional para realizar o monitoramento de indivíduos e Estados considerados como ameaça à segurança nacional. Os casos de ataques cibernéticos que representariam uma guerra cibernéticas são muito menos recorrentes e representam uma demonstração de força ou capacidade tecnológica muito maior do que o monitoramento de dados, como demonstram os três casos analisados. A diferenciação fica mais complicada a partir do momento em que o recolhimento de dados deixar de ter como objetivo único a segurança nacional e passa a visar o roubo de informações vitais, como segredos militares e o conhecimento tecnológico. Em comum, a espionagem e a guerra cibernética possuem o emprego de grandes recursos tecnológicos (AMORIM, 2013).

3 ESTADOS UNIDOS E O BRASIL NO ESPAÇO CIBERNÉTICO

3.1 Os Estados Unidos da América

Os casos analisados foram escolhidos devido à relevância e o impacto no Sistema Internacional. A história cibernética é mais antiga do que os acontecimentos explorados no capítulo anterior, porém é possível perceber que os principais casos ocorreram na última década e isto se dá devido à segurança cibernética ser um campo recente e em desenvolvimento nas relações internacionais. A tendência é que esse campo continue se desenvolvendo e cada vez mais ganhe a atenção, não só dos Estados mais avançados militarmente, mas também de Estados com menos relevância internacional no campo militar. Este capítulo faz uma análise de como os Estados Unidos da América, maior potência atual e país que é referência no campo militar, e o Brasil, país historicamente pacífico e conhecido pelo uso do *soft power*, estão lidando interna e externamente com a questão da segurança cibernética.

Os Estados Unidos passam a dar uma maior importância ao espaço cibernético no século XXI depois de dois acontecimentos, primeiro os ataques terroristas em Nova Iorque e Washington em 11 de setembro de 2001 e segundo os acontecimentos na Estônia em 2007. Como consequência dos ataques de 2001 o governo americano criou o Departamento de Segurança Interna dos Estados Unidos, que tinha como uma das funções a criação de um plano nacional de segurança para infraestruturas chaves do país. A partir desta iniciativa, em 2003, nasceu a Estratégia Nacional para Segurança do Espaço Cibernético (BERWANGER, 2015). Este documento é complementar à Estratégia Nacional de Proteção Física de Infraestruturas Críticas e tem como propósito incentivar e coordenar para que o governo federal, estados, governos locais, o setor privado e o povo americano trabalhem em conjunto para proteger os mais abrangentes ramos da defesa cibernética nacional (USA, 2003).

> The National Strategy to Secure Cyberspace was developed in close collaboration with key sectors of the economy that rely on cyberspace, state and local governments, colleges and universities, and concerned organizations. Town hall meetings were held around the country, and fifty-three clusters of key questions were published to spark public debate. In addition, a draft version of the National Strategy to Secure Cyberspace was shared with the Nation for public comment. The response has been overwhelming. The public-private

> partnerships that formed in response to the President's call have developed their own strategies to protect the parts of cyberspace on which they rely. This unique partnership and process was and will continue to be necessary because the majority of the country's cyber resources are controlled by entities outside of government. For the National Strategy to Secure Cyberspace to work it must be a plan in which a broad cross section of the country is both invested and committed. Accordingly, the dialogue about how we secure cyberspace will continue. The National Strategy to Secure Cyberspace identifies five national priorities that will help us achieve this ambitious goal. These are: (1) a national cyberspace security response system; (2) a national cyberspace security threat and vulnerability reduction program; (3) a national cyberspace security awareness and training program; (4) securing governments' cyberspace; and, (5) national security and international cyberspace security cooperation. These five priorities will serve to prevent, deter, and protect against attacks. In addition, they also create a process for minimizing the damage and recovering from attacks that do occur (USA, 2003, p. 53).

É possível apontar pela conclusão da Estratégia Nacional a importância que o governo norte americano dá à parceira público-privada com empresas, centros de pesquisas e universidades. A parceria é importante para lidar com problemas de coordenação, aumentar a consciência, treinamento, melhorias tecnológicas, correção de vulnerabilidade e operações de recuperação. O governo reconhece que o setor privado é mais bem equipado e estruturado para lidar com ameaças cibernéticas, porém há situações em que a resposta governamental é mais apropriada, como a realização de ataques, proteção de redes e sistemas críticos para a segurança nacional, indicações e avisos e proteção contra ataques capazes de causar danos que afetem a economia (USA, 2003).

O trecho da conclusão em destaque cita ainda as cinco prioridades nacionais, entre elas, a número 5, a Segurança Nacional e a Cooperação pela Segurança do Espaço cibernético Internacional que identifica seis iniciativas para fortalecer a segurança nacional e a cooperação internacional, são elas: 1) Fortalecer os esforços de contrainteligência cibernética; 2) Aprimorar as capacidades de atribuição de ataques e reações; 3) Aprimorar a coordenação de respostas aos ataques cibernéticos em parceria com a comunidade americana para a segurança nacional; 4) Trabalhar com a indústria e as Organizações Internacionais para facilitar o diálogo e parcerias entre os setores públicos e privados internacionais focados na proteção da infraestrutura de informação e promover a "cultura de segurança" global; 5) Promover o estabelecimento de redes nacionais e internacionais de monitoramento e alarme para detectar e prevenir ataques cibernéticos; e 6) Encorajar outras nações a aderirem à Convenção de

Budapeste, também conhecida como Convenção sobre o Cibercrime, ou assegurar que suas leis e procedimentos sejam pelo menos compreensivos (USA, 2003).

Em resposta aos acontecimentos de 2007 na Estônia o governo americano lançou o *Comprehensive National Cyber Initiative* (CNCI), um conjunto de 12 iniciativas com estratégias para a proteção dos sistemas nacionais contra ameaças imediatas e também com uma visão sobre possíveis ameaças futuras. O CNCI continha diretrizes para o governo federal se preparar para a ascensão de novas modalidades de ataques e estar sempre um passo à frente de possíveis adversários cibernéticos (BERWANGER, 2015).

> Initiative #8. Expand cyber education. While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet this challenge (USA, 2009, p. 4).

Entre as iniciativas propostas estava a expansão do investimento em educação sobre a segurança cibernética. Havia um reconhecimento de que os Estados Unidos não contavam com um número suficiente de especialistas em segurança no espaço cibernético e precisariam de pessoas qualificadas para lidar com a expansão do campo. A CNCI chegou à conclusão de que seria necessário um esforço semelhante ao incentivo que ocorreu na década de 1950 nas áreas de matemática e ciências para o desenvolvimento acadêmico do assunto (USA, 2009). O incentivo continua a ocorrer atualmente, tanto que no orçamento presidencial para o ano de 2017 está destacado um valor de 62 milhões de dólares direcionados para suprir a falta de mão de obra qualificada, criando um programa de reservistas para a segurança cibernética e expandindo os programas educacionais em segurança cibernética em instituições pelo país (USA, 2016).

No ano de 2010 o Pentágono, departamento de defesa dos Estados Unidos da América, reconheceu formalmente o espaço cibernético como um novo domínio da

guerra. Segundo William J. Lynn (2011), ex vice-secretário de defesa dos Estados Unidos, o espaço cibernético tornou-se tão crítico para as operações militares americanas como a terra, o mar, o ar e o espaço. Como parte da nova estratégia de defesa cibernética foi criado o *Cyber Command*, dentro do Departamento de Defesa. O *Cyber Command* tem três missões. A primeira é comandar a proteção diária de toda a rede de defesa e apoiar operações militares e de contraterrorismo que ocorram no espaço cibernético. A segunda é fornecer uma maneira transparente e responsável de lidar com os recursos militares destinados ao espaço cibernético. A sua terceira missão é trabalhar com uma variedade de parceiros, dentro e fora do governo americano, como nações aliada e empresas. As três missões trabalham junto com os principais elementos da estratégia americana para o espaço cibernético que são: desenvolver táticas organizacionais para treinar, equipar e comandar forças de defesa cibernéticas; implantar camadas de proteção com uma forte presença de defesas ativas; usar capacidades militares para apoiar esforços de proteção de redes de outros departamentos responsáveis por infraestruturas críticas dos EUA; desenvolver defesas coletivas com seus aliados; e investir em rápido desenvolvimento de novas tecnologias de defesa cibernética (LYNN, 2011).

Mais recentemente, no ano de 2015, o Departamento de Defesa (DoD) norte americano apresentou a sua estratégia cibernética, a *Department of Defense Cyber Strategy* (DoDCS), com o objetivo de guiar o desenvolvimento das suas forças cibernéticas e fortalecer sua defesa e postura de dissuasão, postura essa que o Departamento de Defesa busca alcançar através de um conjunto de ações, entre elas declarações públicas, indicações e avisos sobre suas capacidades, postura defensiva e procedimentos efetivos de respostas (USA, 2015). O Departamento de Defesa possui três principais missões cibernéticas: defender a rede, sistemas e informações do DoD; defender o território e os interesses americanos contra ataques cibernéticos com consequências significantes e fornecer suporte para operações militares e planos de contingência (USA, 2015).

O DoDCS é um guia para o desenvolvimento da *Cyber Mission Force* (CMF), unidade que será responsável pela defesa cibernética do Departamento de Defesa. O CMF quando totalmente implementado terá um total de 133 times que serão compostos

por um total de 6.187 pessoas e um investimento inicial aproximado de 2 bilhões de dólares (USA, 2015). Em 10 de junho de 2016, 46 times já estavam completamente operacionais, com 4.684 pessoas trabalhando para realizar as três missões principais do Departamento (GARAMONE, 2016).

O documento destaca ainda a importância do setor privado para o DoD e a defesa cibernética. O setor privado é dono e gerencia mais 90% de toda a rede e infraestrutura do espaço cibernético, portanto representa a primeira linha de defesa. Segundo DoDCS o passo mais importante para aprimorar a defesa cibernética norte americana é as companhias privadas priorizarem a defesa de suas redes e arquivos sensíveis e investirem na sua própria segurança cibernética. Com o intuito de atrair os melhores talentos, ideias e tecnologias para o serviço público o Departamento tem que manter uma forte ligação com o setor privado e as instituições de pesquisa, já que esses desenvolvem e constroem as redes cibernéticas, são provedores de serviços de segurança e desenvolvem capacidades avançadas de defesa (USA, 2015).

> As DoD builds its Cyber Mission Force and overall capabilities, DoD assumes that the deterrence of cyberattacks on U.S. interests will not be achieved through the articulation of cyber policies alone, but through the totality of U.S. actions, including declaratory policy, substantial indications and warning capabilities, defensive posture, effective response procedures, and the overall resiliency of U.S. networks and systems. The deterrence of state and non-state groups in cyberspace will thus require the focused attention of multiple U.S. government departments and agencies. The Department of Defense has a number of specific roles to play in this equation. Deterrence is partially a function of perception. It works by convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary's attack will succeed. The United States must be able to declare or display effective response capabilities to deter an adversary from initiating an attack; develop effective defensive capabilities to deny a potential attack from succeeding; and strengthen the overall resilience of U.S. systems to withstand a potential attack if it penetrates the United States' defenses. In addition, the United States requires strong intelligence, forensics, and indications and warning capabilities to reduce anonymity in cyberspace and increase confidence in attribution (USA, 2015, p. 10).

A política de dissuasão, ou intimidação, tem papel crucial na estratégia cibernética norte americana e funciona na base da percepção e do convencimento, política que ficou famosa na Guerra Fria, com a dissuasão nuclear. Através de declarações públicas, posturas defensivas, indicações e avisos de capacidade e procedimentos eficazes de respostas os EUA buscam convencer potenciais adversários

que estes sofrerão graves consequências ao realizar um ataque contra o Estados Unidos e os americanos (USA, 2015).

Wei (2015), listou os principais desafios para uma nação alcançar com sucesso a política de dissuasão cibernética. O primeiro é o problema de atribuição. Para a intimidação ser bem sucedida, potenciais agressores precisam da noção de que suas identidades serão expostas e de que sofrerão retaliações. Caso o ataque seja atribuído à outra fonte ou a retaliação ocorra de forma equivocada a lógica da intimidação perderá força e poderá até resultar em um novo inimigo.

A retaliação, como qualquer outro ataque cibernético, utiliza as vulnerabilidades de programas e redes, e essas são corrigidas em curto tempo após sua descoberta, dificilmente falhas são exploradas mais de um vez, assim ataques cibernéticos muitas vezes se tornam armas de apenas uma utilização. Conforme novos ataques ocorrem, mais vulnerabilidades são descobertas e corrigidas, tornando mais complexa e custosa a retaliação (WEI, 2015).

Outra preocupação é evitar a intensificação da situação. A natureza, a escolha e em quanto tempo ocorrerá a retaliação afetarão o modo como a mensagem vai ser recebida pelo agressor. Dada a complexidade de rastrear a fonte do ataque, pode ocorrer um atraso significativo entre a agressão e a ato retaliatório. No momento em que a resposta for percebida pelo agressor, pode ter se passado meses do ataque original, e a retaliação corre o risco de ser percebida como arbitrária e desconexa (WEI, 2015).

O envolvimento de atores não estatais em ataques cibernéticos constitui o último ponto levantado por Wei (2015). Retaliações contra atores não estatais, como grupos como *LulzSec* e *Anonymous*, muitas vezes não valem a pena. A ação pode ser bem sucedida em danificar os sistemas de computadores dos grupos, porem se reequipar exigiria baixos custos. Caso um ator não estatal esteja protegido e acolhido por um Estado, não é legalmente claro se o Estado pode ser responsabilizado pelas ações do grupo. A escolha por retaliação pode resultar em outra ação retaliatória, dessa vez por parte do Estado que acolhe o ator não estatal (WEI, 2015).

Como parte do orçamento presidencial americano que é enviado anualmente para o congresso, o presidente Barack Obama determinou por meio do *Cybersecurity National Action Plan* (CNAP) um montante de mais de 19 bilhões de dólares para o ano de 2017 destinado à segurança cibernética, um aumento de 35% em relação aos gastos de 2016. O CNAP visa aumentar a capacidade da segurança cibernética do governo federal e do ecossistema cibernético nacional como um todo. O plano coloca em prática uma estratégia de longo prazo para aumentar a conscientização para defesa em relação à segurança cibernética. Desse total, 7 bilhões estão destinados à estratégia do Departamento de Defesa, e em particular ao *Cyber Mission Force* (USA, 2016).

> The President's Cybersecurity National Action Plan (CNAP) is the capstone of more than seven years of determined effort by this Administration, building upon lessons learned from cybersecurity trends, threats, and intrusions. This plan directs the Federal Government to take new action now and fosters the conditions required for long-term improvements in our approach to cybersecurity across the Federal Government, the private sector, and our personal lives (USA, 2016).

Entre as principais ações do CNAP estão a criação da Comissão para o Reforço da Segurança cibernética, que junta especialistas de ponta de fora do governo nas áreas de estratégia, negócios e técnicos para realizar recomendações em como usar novas soluções técnicas e práticas para melhor proteger a privacidade e a segurança pública. Trabalha na conscientização da população para melhor proteger suas contas *online* com a utilização de protocolos adicionais de segurança, como utilização de digitais, e trabalha em conjunto com as principais empresas de tecnologia, como Google, Facebook e Microsoft (USA, 2016).

3.2 O Brasil

No Brasil, o espaço cibernético sofre com uma variedade de ameaças, que vão desde golpes bancários a usuários até a espionagem internacional. Porém o debate sobre a militarização do espaço cibernético é mais recente (MUGGAH; DINIZ; GLENNY, 2014). Em 2008 o Brasil lançou a Estratégia Nacional de Defesa (END), aprovado pelo decreto 6.703, de 18 de dezembro. A END visa reorganizar e reorientar as Forças Armadas e remodelar a indústria de defesa com o objetivo de ter sob domínio

nacional as tecnologias mais avançadas e ainda ações estratégicas de modernização da estrutura nacional de defesa. Na END, o Brasil reconhece o setor cibernético como um dos três setores decisivos para a defesa nacional, junto com o espacial e o nuclear e designou a criação de uma organização responsável pelo desenvolvimento e capacitação cibernética em âmbito industrial e militar (BRASIL, 2008).

> As capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. Contemplarão o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar (BRASIL, 2008, p. 33).

A Estratégia Nacional destacou a importância do desenvolvimento de conhecimento próprio para assim ser possível visualizar um Brasil independente de tecnologias estrangeira, é prioritário então uma forte relação entre centros de pesquisa, indústria e as forças militares (COELHO, 2012).

Entretanto, Celles (2015) destacou a descentralização que existe na estratégia cibernética brasileira. Diferente dos setores nuclear e espacial, a segurança cibernética não possui uma agência central. Enquanto a Comissão Nacional de Energia Nuclear (CNEN) é a agência federal responsável por pesquisa, desenvolvimento, programas de energia nuclear para uso civil e também militar, tendo participação no desenvolvimento do propulsor nuclear brasileiro para submarinos. O setor espacial também possui agência própria, a Agência Espacial Brasileira (AEB), que segundo seu *website* é "[...] a instituição responsável por formular, coordenar e executar a Política Espacial Brasileira. Desde a sua criação, em fevereiro de 1994, a Agência trabalha para empreender os esforços do governo brasileiro na promoção da autonomia do setor espacial". Porém falta ao setor cibernético uma agência federal com autoridade central para organizar e debater estratégias nacionais de uso do espaço cibernético. Existem múltiplas agências envolvidas com a segurança cibernética. Como exemplo temos o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal, no âmbito da presidência da Presidência da República (CTIR Gov), o Centro de Monitoramento do Serviço a Crimes Cibernéticos da Polícia Federal e o Centro de Defesa Cibernética (CDCiber) do Exército Brasileiro, esse que

nos últimos anos tem se destacado como um possível catalisador das ações de defesa cibernética no Brasil (CORDEIRO, 2015).

Por causa da descentralização existente no setor cibernético não há uma autoridade central para delegar tarefas, esforços e ditar caminhos a serem seguidos por organizações governamentais e privadas. A falta de definição das responsabilidades também é consequência da descentralização do setor cibernético. Assim, não há uma definição sobre quem será o responsável pela retaliação, caso necessário, de um ataque à redes governamentais ou privadas do Brasil (CORDEIRO, 2015).

O espaço cibernético ganhou mais visibilidade nacional em 2013 após as revelações de Edward Snowden de que o Brasil era alvo de espionagem da NSA, agência americana de segurança. Diversos alvos brasileiros foram revelados, incluindo a ex-presidente da república, Dilma Rousseff, e membros do alto escalão de seu governo (MUGGAH; DINIZ; GLENNY, 2014). Em uma reação diplomática imediata ao teor dos vazamentos o governo brasileiro cancelou a visita presidencial que ocorreria em outubro daquele ano. Dilma Roussef ainda utilizou o seu discurso de abertura da Assembleia Geral da ONU para criticar a espionagem da NSA (FERREIRA; CANABARRO, 2015).

> Quero trazer à consideração das delegações uma questão a qual atribuo a maior relevância e gravidade.
>
> Recentes revelações sobre as atividades de uma rede global de espionagem eletrônica provocaram indignação e repúdio em amplos setores da opinião pública mundial.
>
> No Brasil, a situação foi ainda mais grave, pois aparecemos como alvo dessa intrusão. Dados pessoais de cidadãos foram indiscriminadamente objeto de interceptação. Informações empresariais – muitas vezes, de alto valor econômico e mesmo estratégico - estiveram na mira da espionagem. Também representações diplomáticas brasileiras, entre elas a Missão Permanente junto às Nações Unidas e a própria Presidência da República tiveram suas comunicações interceptadas.
>
> Imiscuir-se dessa forma na vida de outros países fere o Direito Internacional e afronta os princípios que devem reger as relações entre eles, sobretudo, entre nações amigas. Jamais pode uma soberania firmar-se em detrimento de outra soberania. Jamais pode o direito à segurança dos cidadãos de um país ser garantido mediante a violação de direitos humanos e civis fundamentais dos cidadãos de outro país (ROUSEFF, 2013).

Em 2012, o Brasil lançou a Política Cibernética de Defesa que tem como objetivos assegurar o uso do espaço cibernético pelas Forças Armadas, impedir a

utilização do espaço cibernético contra os interesses da defesa nacional, capacitar recursos humanos para a condução das atividades do setor cibernético e colaborar com a produção de conhecimento na área (BRASIL, 2012).

> São objetivos da Política Cibernética de Defesa: a) assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas (FA) e impedir ou dificultar sua utilização contra interesses da Defesa Nacional; b) capacitar e gerir talentos humanos necessários à condução das atividades do Setor Cibernético (St Ciber) no âmbito do MD; c) colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (SINDE) e para os órgãos de governo envolvidos com a SIC e Segurança Cibernética, em especial o Gabinete de Segurança Institucional da Presidência da República (GSI/PR); d) desenvolver e manter atualizada a doutrina de emprego do St Ciber; e) implementar medidas que contribuam para a Gestão da SIC no âmbito do MD; f) adequar as estruturas de C,T&I das três Forças e implementar atividades de pesquisa e desenvolvimento para atender às necessidades do St Ciber; g) definir os princípios básicos que norteiem a criação de legislação e normas específicas para o emprego no St Ciber; h) cooperar com o esforço de mobilização nacional e militar para assegurar a capacidade operacional e, em consequência, a capacidade dissuasória do St Ciber; e i) contribuir para a segurança dos ativos de informação da Administração Pública Federal (APF), no que se refere à Segurança Cibernética, situados fora do âmbito do MD (BRASIL, 2012, p. 13).

A portaria 3.028/2012 do Ministério da Defesa atribui a defesa cibernética ao Exército Brasileiro por meio do Centro de Defesa Cibernética do Ministério da Defesa (CDCiber). O CDCiber tem como objetivo a capacitação de militares na área de ciberdefesa, desenvolvimentos de sistemas e a parceria com a indústria nacional (BRASIL, 2012). Este centro desempenhou papel importante em grande eventos, como a Rio +20, Copa das Confederações de 2013, Copa do Mundo de 2014 (GRAÇA, 2014). Quando o CDCiber foi lançado, em 2010, houve uma liberação de 400 milhões de reais para ser utilizado em um período de 4 anos, que começaram a contar em 2012, a partir da inauguração do centro. Da criação do CDCiber até o final de 2015 já havia se gastado 190 milhões de reais com a implementação e atividades operacionais do Centro de Defesa Cibernética. Para 2016 é previsto um investimento de 36 milhões de reais por parte do Ministério da Defesa, investimento que fica próximo à previsão anual orçamentária de 42 milhões de reais para o CDCiber, totalizando 840 milhões de reais de 2015 até 2035 (FRAGOLA, 2016). O órgão ainda não possui sede própria e conta com cerca de 300 profissionais atuando diretamente para o funcionamento do centro.

Segundo o general José Carlos dos Santos, ex chefe do CDCiber, os programas militares cibernéticos do Brasil possuem características defensivas. Santos compara a estratégia cibernética brasileira com a estratégia nuclear. De acordo com o general, mesmo o Brasil não possuindo armas nucleares, o exército possui uma equipe de defesa preparada para atuar contra os ataques deste tipo, o que também acontece com as armas cibernéticas, que podem ser desenvolvidas pelo exército brasileiro, mas, segundo Santos, "seu uso não condiz com a postura pacífica do país" (BERNARDO, 2014).

> O Brasil é pacífico por tradição e por convicção. Vive em paz com seus vizinhos. Rege suas relações internacionais, dentre outros, pelos princípios constitucionais da não intervenção, defesa da paz, solução pacífica dos conflitos e democracia. Essa vocação para a convivência harmônica, tanto interna como externa, é parte da identidade nacional e um valor a ser conservado pelo povo brasileiro. O Brasil ascenderá ao primeiro plano no cenário internacional sem buscar hegemonia. O povo brasileiro não deseja exercer domínio sobre outros povos. Quer que o Brasil se engrandeça sem imperar (BRASIL, 2008, p. 1).

O trecho acima é o primeiro parágrafo da Estratégia Nacional de Defesa e vai de acordo com as palavras de José Carlos do Santos, evidenciando o caráter pacífico como norteador de todas as políticas da estratégia de defesa brasileira.

3.3 Semelhanças e diferenças entre Brasil e Estados Unidos

Os Estados Unidos são a maior potência da atualidade. Seja na área econômica ou na militar. Com a análise dos principais documentos oficiais americanos sobre a defesa cibernética, como a Estratégia Nacional para Segurança do Espaço Cibernético, DoDCS e CNAP, é possível destacar que os EUA estão dispostos a defender sua posição como potência dominante também no espaço cibernético. Os EUA buscam defender suas infraestruturas críticas, aumentar a participação do setor privado na segurança cibernética, proteger as informações de seus cidadãos e aprimorar uma força capaz de atacar qualquer outra rede mundial e retaliar ataques direcionados ao seu governo, suas empresas, infraestruturas ou cidadãos.

No Brasil o espaço cibernético ganhou mais visibilidade durante a preparação para os grande eventos que ocorreram no país a partir de 2012 com a Rio +20, passando pela Copa das Confederações em 2013, Copa do Mundo em 2014 e por

último os jogos olímpicos Rio 2016, porém as principais preocupações eram com a desconfiguração de sites oficiais, conhecidos como pichações. Antes desses eventos o espaço cibernético era contemplado com investimentos do Ministério da Defesa mas voltados para telecomunicações, aeroespacial e estruturas de tecnologia da informação (FRAGOLA, 2016).

Para Fragola (2016), o maior legado dos eventos para a segurança cibernética foi a criação do CDCiber. O centro teve um papel importante na busca pela descentralização da defesa cibernética e é líder na execução de projetos estratégicos na área, como a criação da Escola Nacional de Defesa Cibernética, criada pela Portaria normativa Nº 2.777 do Ministério da Defesa de outubro de 2014, em parceria com a Universidade de Brasília. (MATSUURA, 2015).

Outro ponto que aparece como grande divergência entre as políticas americanas e brasileiras é a atenção dada ao setor privado. É da natureza dos EUA dar mais atenção à empresas e centros de pesquisa, principalmente no setor cibernético, uma vez que as principais empresas de tecnologia do mundo são americanas, e essas possuem um papel principal na segurança cibernética (USA, 2015).

No Brasil, a base da defesa cibernética é militarizada, mesmo o CDCiber mantendo projetos com a Universidade de Brasília e o Serviço Federal de Processamento de Dados (SERPRO), o foco principal é a defesa nacional. Há uma ausência de políticas que estimulem a troca de informações e de boas práticas para a segurança cibernética com foco nas infraestruturas críticas e ações civis. Falta uma maior comunicação e integração entre o CDCiber e programas de fomento a pesquisa e desenvolvimento do Estado, como o Inova da Financiadora de Estudos e Projetos (FINEP), que tem como objetivo a inovação de diversas áreas de interesse para o país, incluindo áreas diretamente ligadas ao espaço cibernético, como a aerodefesa, energia e telecom (FRAGOLA, 2016).

A participação popular na segurança cibernética do Brasil é assunto a se destacar. A população teve grande participação no Marco Civil da Internet, aprovado em 2014, conhecido como a "constituição da internet", que tem entre seus principais temas a neutralidade da rede, privacidade na web e registros de acessos (BRASIL, 2014). A

participação popular na segurança cibernética também é destaque nas eleições brasileiras. O TSE promove testes públicos de segurança da urna eletrônica em anos de eleição. Os testes públicos são abertos para quem quiser se inscrever e segundo o *website* do próprio TSE " tem por objetivo fortalecer a confiabilidade, a transparência e a segurança da captação e da apuração dos votos e propiciar melhorias no processo eleitoral" (BRASIL, 2016).

Em relação a tratados e acordos internacionais no setor cibernético, a Convenção de Budapeste de 2001 aparece como um dos principais esforços da normatização internacional dos cibercrimes. A convenção foi desenvolvida pelo Conselho Europeu, mas sempre visando o cenário internacional (CLOUGH, 2012).

> Although developed by the CoE, it was always intended for the Convention and its Protocol to apply at a world-wide level. These instruments now serve an increasing number of countries around the world as a guideline for the preparation of national legislation, and as a global framework for cooperation against cybercrime (COUNCIL OF EUROPE, 2009, p. 5).

O principal objetivo da Convenção é combater crimes cibernéticos através da concordância das legislações internacionais e da cooperação internacional. A Convenção exige o estabelecimento de procedimentos domésticos de detecção e investigação de crimes cibernéticos, e o colhimento de evidências de qualquer ofensa criminal. Define os crimes cibernéticos em quatro categorias: fraude; pornografia infantil; violação de direitos autorais, *hacking* e interceptação ilegal de dados; e interferências de sistemas que comprometem a integridade e disponibilidade da rede. E por último estabelece um sistema rápido e efetivo para a cooperação internacional, incluindo a permissão para que autoridades de um país coletem evidencias cibernéticas em outros países (ARCHICK, 2004).

Os Estados Unidos são signatários e colaboraram com o desenvolvimento da Convenção, sendo ratificada em 2006 e entrando em vigor no dia 1º de janeiro de 2007. O Brasil, por meio de uma pró memória enviada à Comissão da Nações Unidas de Prevenção ao Crime e Justiça Criminal, declarou que não teve a oportunidade de contribuir nas negociações e considera que nenhum fórum multilateral ou regional pode substituir as Nações Unidas (BRASIL, 2015).

> While Brazil appreciates that international instruments to counter this challenge have already been signed and implemented, it also considers that a multilateral

> legal framework would be the best possible response by the international community. Brazil recognizes the fact that the members of the Council of Europe and a number of other countries consider that the Budapest Convention is already the global response. In Brazil's view, however, the approach taken by this Convention in its Section 1 is not appropriate. Brazil does not see the rationale to single out some particular forms of cybercrime for definition and inclusion in the Convention. Moreover, Brazil did not have an opportunity to contribute to the negotiations, and it considers that no regional or international forum, no matter how important and representative it could be, is a substitute for the United Nations as the legitimate forum for the negotiation of global legal frameworks (BRASIL, 2015, p.2).

Neste capítulo é possível observar que os EUA e o Brasil possuem objetivos distintos em relação à segurança cibernética e coerentes com suas estratégias internacionais. Os Estados Unidos já possuem uma estratégia de ciberdefesa bem estruturada e buscam ser a maior potência cibernética, capaz de atacar qualquer rede e qualquer computador no globo, de se defender de ataques, seja de países ou de atores não estatais e também de retaliar qualquer ação que vá de encontro com os seus interesses. O Brasil mostrou uma preocupação maior em relação ao espaço cibernético com os grandes eventos que sediou, com a privacidade das redes de comunicação do governo e da formação de uma base sólida de defesa cibernética com o CDCiber. Em comum, os dois países têm o discurso da securitização e da importância da defesa cibernética, que vão de acordo com a teoria de securitização da Escola de Copenhagen, como citado no primeiro capítulo.

Por fim, uma outra diferença percebida pelo autor desta pesquisa é a disponibilidade e facilidade de acesso a informações oficiais em relação às políticas de defesa cibernéticas dos EUA e do Brasil. As principais informações sobre documentos, políticas, ações e discursos americanos foram localizados com certa facilidade em pesquisas nos sites como os da Casa Branca, do Departamento de Defesa e das Forças Armadas americanas. No caso brasileiro a maioria das informações oficiais encontradas foram dos decretos presidenciais, notícias e entrevistas concedidas por oficias à portais de notícias. Existem poucas informações oficiais recentes em relação ao trabalho realizado diariamente pelos órgãos de defesa cibernética do país e o seu orçamento. É de se destacar a falta de um *website* oficial do Centro de Defesa Cibernética do Exército Brasileiro. O único portal oficial dedicado exclusivamente à defesa cibernética é o Instituto de Defesa Cibernética, que em parceria com a Universidade de Brasília busca reunir e disponibilizar pesquisas e cursos para o

desenvolvimento de recurso humano na área de segurança cibernética, porém o site encontra-se claramente desatualizado e incompleto.

CONCLUSÃO

No primeiro capítulo houve uma exposição da literatura das Relações Internacionais na área de segurança cibernética. O levantamento literário feito por Reardon e Choucri (2012), foi comparado com artigos da academia brasileira e foi possível constatar que há uma tendência em se analisar o cenário cibernético nas Relações Internacionais com base no conceito de securitização desenvolvido por Buzan, Waever e Wilse (1998), da Escola de Copenhagen. Como demonstrando no terceiro capítulo, realmente há uma militarização e institucionalização do espaço cibernético por parte dos Estados Unidos e mais recentemente do Brasil.

Como analisado no segundo capítulo, o caso da Estônia em 2007 foi o primeiro ataque cibernético a levantar uma preocupação global sobre as reais capacidades de um ciberataque. À época a Estônia já era considerada como um dos países mais conectados do mundo, e os ataques cibernéticos não mudaram essa postura. Atualmente, quase 10 anos após os ataques, todas as transações do governo estoniano ou serviços são realizados online, desde o pagamento de impostos até o sistema eleitoral, incluindo a votação. Todas as agências governamentais estão online, e a população usufrui de uma comunicação eficiente entre os sistemas. Como era de se esperar o país se dedicou a desenvolver uma defesa cibernética mais robusta, incluindo a formação da primeira aliança cibernética formal, a *Digital 5* (D5), que além da Estônia é formada por Israel, Nova Zelândia, Coréia do Sul e Reino Unido, e tem o objetivo de compartilhar boas práticas governamentais no espaço cibernético e debater sobre as principais tendências do desenvolvimento tecnológico mundial (KHANNA, 2015).

Na última parte dessa pesquisa foi feita uma comparação entre as políticas adotadas pelos Estados Unidos e pelo Brasil e a crescente militarização do espaço cibernético, tanto por parte americana, como brasileira. Essa militarização é decorrente do crescente temor de que o espaço cibernético será utilizado por Estados ou atores não-estatais, para atacar os interesses nacionais. Seja por meio de espionagem ou ataques contra infraestruturas críticas. A constante atualização e modernização do espaço cibernético e a quantidade quase que ilimitada de atores atuantes e anônimos faz com que Estados se preparam para se proteger de ameaças ainda não lhes são

conhecidas. Não é possível saber exatamente como serão as ameaças futuras, mas é importante prestar atenção nas tendências atuais que possam moldar o mundo futuro, é importante frisar que tendências não são inflexíveis, e que muitas outras surgirão com o tempo. Singer e Friedman (2014) chegaram a cinco tendências para o futuro da segurança cibernética.

A primeira é o surgimento da computação de nuvem. Aonde os recursos são gerenciados fora dos controles individuais ou das organizações. Uma nova *startup,* por exemplo, não precisa mais se preocupar em comprar e gerenciar seu próprio servidor, ou espaço de armazenamento. Esses recursos agora podem ser alugados de terceiros, em servidores externos, economizando investimentos em *hardware* e ocupação de espaço físico. A principal importância da chamada "nuvem" para o futuro da segurança cibernética é a importância que as companhias controladoras dos dados ganham em detrimento dos computadores de indivíduos e empresas. Há um aumento na segurança da informação, uma vez que companhias como Google e Microsoft, especialidas em nuvem, possuem engenheiros de segurança mais bem preparados que a maioria das empresas contratantes (SINGER; FRIEDMAN, 2014).

Armazenamento e computação mais baratos e acessíveis inspirará novos usos de coleta e análise de dados, o que segundo Singer e Friedman (2014), leva à segunda tendência, a "*Big Data*". Com o aumento dos dados disponíveis no espaço cibernético, novos mecanismos de análise são necessários para os entender e analisar, o que vem mudando os entendimentos que temos sobre a rede. Desde a busca por terroristas por parte da NSA, ao Netflix, que utiliza os dados com as preferências de seus usuários para se relacionar com o mercado de uma maneira completamente nova, utilizando as informações coletadas para produzir suas próprias séries. A *Big Data* também é causa de preocupações. A revelação da coleção de dados da população por parte da NSA causou um grande escândalo mundial em relação à privacidade, com implicações que vão desde a confiança da população e de outros países no governo americano até a ações de combate ao terrorismo. Mais data e melhores ferramentas para interpretá-las geram grande conhecimento, mas podem também romper barreiras, sociais, legais e éticas (SINGER; FRIEDMAN, 2014).

Tecnologia melhor e mais barata tem causado uma outra tendência, a chamada "revolução móvel". Aparelhos celulares não são novidade, porém a popularização dos *smartphones*, aparelhos com acesso à internet, tem a capacidade de transformar o mundo com a popularização do acesso à informação, especialmente nos país em desenvolvimento. Porém essa popularização gera também uma preocupação em relação à segurança cibernética, já que o espaço cibernético alcançou lugares menos capazes de arcar com soluções de ponta para a segurança (SINGER; FRIEDMAN, 2014).

Há uma mudança demográfica em relação aos usuários do espaço cibernético, o que resulta na quarta tendência apontada por Singer e Friedman (2014). Há uma quantidade cada vez maior de usuários não ocidentais no espaço cibernético, o que aumenta o caráter democrático da rede, mas também causa rupturas. A internet foi criada majoritariamente por cientistas americanos, que a moldaram com base em conexão, compartilhamento e liberdade. Porém cada vez mais tem ocorrido uma mudança nessa visão, com o risco de a internet se tornar cada vez mais dividida. Há um crescente número de países, que como a China, criam uma internet própria, moldada de acordo com os interesses do regime (SINGER; FRIEDMAN, 2014).

A última tendência tem sérias implicações na segurança cibernética. Um futuro em que o cibernético e o físico vão estar interligados, sistemas digitais estarão incorporados no mundo real, em uma tendência que é conhecida como a Internet das Coisas. Este conceito tem a finalidade de conectar aparelhos do dia-a-dia. Aparelhos que vão desde celulares a carros já possuem sistemas de computadores integrados, a ideia é que os mais diversos aparelhos se comuniquem entre si e que os dados armazenados sejam utilizados por sistemas de trânsito, de segurança, de saúde, entre outros, a um ponto em que tudo esteja conectado e em sintonia. Com uma maior interconexão de diversos sistemas os ataques cibernéticos serão capazes de agir cada vez mais profundamente nas atividades cotidianas (SINGER; FRIEDMAN, 2014).

Cada uma dessas tendências do espaço cibernético traz novos desafios, tanto para a população em geral quanto para governos, mercados e para as Relações Internacionais. A velocidade com que o espaço cibernético evolui pode ser intimidadora

e o futuro cheio de incertezas, porém é necessário uma busca constante por evolução e aperfeiçoamento das boas práticas no espaço cibernético.

Como demonstrado, o movimento de securitização foi iniciado pelos Estados Unidos na década de 90. Por ser a maior potência mundial é comum que os outros países sigam seus movimentos, o que ocorreu com o Brasil. Entretanto, segundo a Escola de Copenhagen, a crescente securitização leva à militarização. Os Estados Unidos estão seguindo esta ordem, com um discurso sobre os perigos do espaço cibernético que vem desde a década de 90, seguido pela militarização com a criação de regimentos dedicados aos conflitos cibernéticos e o crescente investimento por parte do Departamento de Defesa. Entretanto, no Brasil até os anos 2000 não se falava sobre guerras cibernéticas, e os discursos de securitização já foram acompanhados da militarização do espaço cibernético, designando sua responsabilidade ao Exército Brasileiro. A securitização do espaço cibernético é acompanhada por muitos discursos que comparam o espaço cibernético às lógicas tradicionais de segurança, o que não se aplica na realidade. Mesmo com o crescente temor de que o espaço cibernético se torne um grande campo de batalhas entre Estados e também atores não-estatais, é necessário ter a consciência que o espaço cibernético surgiu como uma rede livre, e assim deve permanecer.

REFERÊNCIAS

ACÁCIO, Igor. *Segurança cibernética:* análise sobre a política de defesa brasileiro. 2011, 98 f. Dissertação (Bacharelado) - Relações Internacionais, Universidade Federal Fluminense, Rio de Janeiro 2011.

AMORIM, Celso. Segurança Internacional: novos desafios para o Brasil. *Contexto internacional*, Rio de Janeiro , v. 35, n. 1, p. 287-311, 2013. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292013000100010&lng=en&nrm=iso>. Acesso em: 27 ago. 2016.

ARCHICK, Kristin. C*ybercrime:* the council of europe convention*.* CRS Report for Congress. Washington, Library of Congress, 2004.

ARQUILLA, John; RONFELDT, David. *Cyberwar is coming! Comparative Strategy*. Santa Monica: Rand Publishing, 1993.

AZZOPARDI, Myrna. The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Brief Introduction on Its Treatment of Jus Ad Bellum Norms. *Elsa Malta Law Review*, v. 3, 2013.

BBC BRASIL, *Entenda o Conflito Envolvendo Rússia e Geórgia na Ossétia do Sul.* Disponível em: <http://www.bbc.com/portuguese/reporterbbc/story/2008/08/080808_entenda_ossetia_cg.shtml>. Acesso em: 07 jun. 2016.

BERNARDO, Kaluan. *Nenhum país está preparado para guerra virtual, diz Exército Brasileiro.* Disponível em: <http://embed.olhardigital.uol.com.br/fique_seguro/noticia/o-brasil-esta-preparado-para-uma-guerra-virtual/33307>. Acesso em: 30 ago. 2016.

BERWANGER, Tiago. *O Discurso de Securitização da Cibernética nos Estados Unidos da América no Período entre 2007 e 2015.* 2015*.* 94 f. Dissertação (Bacharelado) - Relações Internacionais, Universidade Federal de Santa Catarina, Paraná, 2015.

BOUSQUET, Antoine. Chaoplexic warfare or the future of military organization. *International Affairs*, v. 84, n. 5, p. 915-929, 2008.

BRASIL. *Entenda o marco civil da internet ponto a ponto.* Disponível em: < http://www.ebc.com.br/tecnologia/2014/04/entenda-o-marco-civil-da-internet-ponto-a-ponto > Acesso em: 27 set. 2016.

BRASIL. *Estratégia Nacional de Defesa*. Brasília, 2008. Disponível em: <http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf >. Acesso em: 04 maio 2016.

BRASIL. *Non-paper submitted by Brazil reflecting its views on the issue of cybercrime.* Commission on Crime Prevention and Criminal Justice. Viena, 2015.

BRASIL. *Política de Defesa Cibernética*. Brasília, 2012. Disponível em: <http://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf >. Acesso em: 04 maio 2016.

BRASIL. *Teste público de segurança do sistema eletrônico de votação 2016*, 2016. Disponível em: < http://www.tse.jus.br/hotSites/testes-publicos-seguranca-2016/> Acesso em: 29 set. 2016.

BRENNER, Susan W. *Cybercrime:* criminal threats from cyberspace. Santa Barbara: ABC-CLIO, 2010.

BROOKING, Emerson; SINGER, Peter Warren. *War goes viral:* how social media is being weaponized across the world. Disponível em: <http://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/>. Acesso em: 05 set. 2016.

CARVALHO, Paulo Sérgio Melo. *A defesa cibernética e as infraestruturas críticas nacionais*. Rio de Janeiro, 24 maio 2011. Disponível em: <http://www.nee.cms.eb.mil.br/attachments/article/101/cibernetica.pdf>. Acesso em: 21 jun. 2016

CAVELTY, Myriam Dunn. The militarisation of cyber security as a source of global tension. *In*: MÖCKLI, Daniel (Org). *Strategic trends 2012:* key developments in global affairs. Zurich: Center for Security Studies (CSS), 2012. Disponível em: < http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Strategic-Trends-2012-Cyber.pdf >. Acesso em: 13 abr. 2016.

CEPIK, Marco; CANABARRO, Diego Rafael; BORNE, Thiago. A securitização do espaço cibernético e o terrorismo: uma abordagem crítica. In: CEPIK, Marco (Org.). *Do 11 de Setembro de 2001 à 'Guerra Contra o Terror'*: reflexões sobre o terrorismo no século XXI. Brasília: IPEA, 2014

CHOUCRI, Nazli. *Co-Evolution of Cyberspace and International Relations:* New Challenges for the Social Sciences. Disponível em: <http://ecir.mit.edu/images/stories/WSSF%20Co-evolution%20of%20cyberspace%20and%20IR%20final.pdf>. Acesso em: 04 maio 2016.

CLARKE, Colin; PORCHE, Isaac. *The online fight against ISIS,* 2016. Disponível em: <https://www.project-syndicate.org/commentary/the-online-fight-against-isis-by-colin-p--clarke-and-isaac-r--porche-iii-2016-04>. Acesso em: 23 set. 2016.

CLARKE, Richard. War from cyberspace. *The National Interest*, Washington, 104, p. 31-36, maio/jun. 2009.

CLOUGH, Jonathan. The council of europe convention on cybercrime: defining crime'in a digital world. *Criminal Law Forum*. p. 363-391. Amsterdã: Springer, 2012.

COELHO, Alessandro Pômpeu. A Estratégia Nacional de Defesa e o setor Cibernético. *Coleção Meira Mattos-Revista das Ciências Militares*. Rio de Janeiro: Exército Brasileiro, 2012.

CORDEIRO, Major Luis Eduardo Pombo Celles. *Brazilian Cyber Power*. Disponível em: <http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2015/2015-1/2015_1_02_pombo-celles_s_eng.pdf>. Acesso em: 05 set. 2016.

CROFT, Adrian; APPS, Peter. *Sites da OTAN sofrem ataque cibernético relacionado à tensão na Criméia,* 2014. Disponível em: <http://br.reuters.com/article/worldNews/idBRSPEA2F00Q20140316>. Acesso em: 13 maio 2016.

DARTNELL, Michael. Weapons of mass instruction: Web activism and the transformation of global security. *Millennium-journal of international studies*, Londres, v. 32, n. 3, p. 477-499, 2003.

DAVIS, Joshua. H*ackers take down the most wired country in europe.* Disponível em: < http://www.wired.com/2007/08/ff-estonia/>. Acesso em: 09 jun. 2016

DEMCHAK, Chris C.; DOMBROWSKI, Peter. Rise of a cybered westphalian age. *Strategic studies quarterly*, Montgomery, 2011, v. 5, n. 1, p. 32-61, 2011.

DER DERIAN, James. The question of information technology in international relations. *Millennium-Journal of International Studies*. Londres, v. 32, n. 3, p. 441-456, 2003.

DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha*. Deconstructing cyber security in brazil*. Instituto Igarapé. Disponível em: < https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf>. Acesso em: 02 jul. 2016.

FARWELL, James; ROHOZINSKI, Rafal. Stuxnet and the future of cyber war. Survival, Nova Iorque, v. 53, n. 1, p. 23-40, 2011.

FERREIRA, Thiago Borne; CANABARRO, Diego Rafael. As reações brasileira ao caso snowden: implicações para o estudo das relações internacionais em um mundo interconectado. *Conjuntura Austral*, Porto Alegra, v. 6, n. 30, p. 50-74. 2015

FRAGOLA, Rodrigo Jonas. *Os próximos passos da estratégia cibernética de defesa do brasil.* Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/21837/Os-Proximos-Passos-da-Estrategia-Cibernetica-de-Defesa-do-Brasil/> Acesso em: 22 set. 2016.

GARAMONE, Jim. *Cyber command deputy details formation of cyber mission force,* 2008. Disponível em: <http://www.defense.gov/News/Article/Article/809904/cyber-command-deputy-details-formation-of-cyber-mission-force> Acesso em: 3 maio 2016.

GOLDMAN, Emily. Introduction: information resources and military performance. *Journal of Strategic Studies.* Londres, v. 27, n. 2 p.195-219, 2004.

GRAÇA, Pedro José Bentes Graça. *O ciberataque como guerra de guerrilha: o caso dos ataques DoS/DDoS à Estónia, Geórgia e ao Google - China.* 2013. 74 f. Dissertação (Mestrado) - Estratégia, Instituto Superior de Ciências Sociais e Políticas. Lisboa, 2013.

GRAÇA, Ronaldo Bach. *Regulação da Guerra Cibernética e o Estado Democrático de Direito no Brasil*. Revista de Direito, Estado e Telecomunicações, p. 63-86, 2014.

HAMMERSLEY, Ben. *Why you should be an e-resident of estonia.* Disponível em: < http://www.wired.co.uk/article/estonia-e-resident>. Acesso em: 09 jun. 2016

HANSEN, Lene.; NISSENBAUM, Helen. Digital disaster, cyber security, and the Copenhagen School*. International studies quarterly*, Londres, v. 53, n. 4, p. 1.155-1.175, dez. 2009.

JENSEN, Eric Talbot. State obligations in cyber operations. *Baltic yearbook of international law*. Provo, v.14, n. 1, p. 71-92, mar. 2014.

KAZ, Roberto. *Petrobras foi alvo de espionagem do governo americano,* 2013. Disponível em: <http://oglobo.globo.com/brasil/petrobras-foi-alvo-de-espionagem-do-governo-americano-9877320> Acesso em: 17 ago. 2016.

KHANNA, Parag. *How small states prepare for cyber-war.* Disponível em: < http://edition.cnn.com/2015/09/02/opinions/estonia-cyber-war/> Acesso em: 06 set. 2016.

KING, Charles. The five-day war. *Foreign Affairs*. Nova Iorque, v. 87, n. 6, p. 2-11, nov/dez. 2008.

LANGNER, Ralph. Stuxnet: dissecting a cyberwarfare weapon. *IEEE Security & Privacy*. Washington, v. 9, n. 3, p. 49-51, 2011.

LOBATO, Luísa Cruz; KENKEL, Kai Michael. *Discourses of cyberspace securitization in Brazil and in the United States*. Rev. bras. polít. int., Brasília , v. 58, n. 2, p. 23-43, 2015 . Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-73292015000200023&lng=en&nrm=iso>. Acesso em: 14 abr. 2016.

LUTTWAK, Edward N., Power relations in the new economy. *Survival.* Londres, *v.* 44, n. 2, p. 7-17, 2002.

LYNN, William J. *The pentagon's cyberstrategy, one year later: defending against the next cyberattack*. Disponível em: <http://www.foreignaffairs.com/articles/68305/williamj-lynn-iii/the-pentagons-cyberstrategy-one-year-later>. Acesso em: 17 jun. 2016.

MARKOF, John. *Before the gunfire, cyberattacks,* 2008. Disponível em: < http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0. Acesso em: 09 jun. 2016.

MATSUURA, Sérgio. *Brasil terá escola nacional de guerra cibernética,* 2015. Disponível em: < http://oglobo.globo.com/sociedade/tecnologia/brasil-tera-escola-nacional-de-defesa-cibernetica-15914957>. Acesso em: 05 maio 2016.

NATO. *The Tallinn manual on international law applicable to cyber warfare*. Cambridge: Cambridge University Press, 2013.
NEWMYER, Jacqueline. The revolution in military affairs with chinese characteristics. *Journal of Strategic Studies*. Londres, v. 33, n. 4, p.483-504, 2010.

OWENS, William; KENNETH, Dam; HERBERT, Lin. *Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities*. Washington: National Academies Press, 2009.

REARDON, Robert; CHOUCRI, Nazli. *The role of cyberspace in International Relations: a view of the literature*. Disponível em < http://ecir.mit.edu/images/stories/Reardon%20and%20Choucri_ISA_2012.pdf>. Acesso em: 06 abr. 2016.

RICHARDS, Jason. *Denial-of-service: The Estonian cyberwar and its implications for US national security*, 2009. Disponível em: <http://www.iar-gwu.org/node/65>. Acesso em: 18 jun. 2016

ROUSEFF, Dilma. *Discurso da Presidenta da República, Dilma Rousseff, na abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas* - Nova Iorque. Disponível em: <http://www2.planalto.gov.br/acompanhe-o-planalto/discursos/discursos-da-presidenta/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua>. Acesso em: 05/09/2016.

RUSSELL, Alec. *CIA plot led to huge blast in Siberian gas pipeline*, 2004. Disponível em: <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html>. Acesso em: 04 mar. 2016.

SCHMITT, Michael. Computer network attack and the use of force in international law: thoughts on a normative framework. *Columbia Journal of transnational law*. Nova Iorque, v. 37, p. 885-937, 1999.

SINGER, Peter W.; FRIEDMAN, Allan. *Cybersecurity:* what everyone needs to know. Oxford: Oxford University Press, 2014.

SPUTNIKNEWS. *Estonia Has No Evidense of Kremlin Involvement in Cyber Attacks.* Disponível em: < https://sputniknews.com/world/2007090676959190/>. Acesso em: 06 jun. 2016.

SWAINE, Jon. *Gerogia:* Russia 'conducting cyber war'*.* Disponível em: <http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> Acesso em: 09 jun. 2016.

TRAYNOR, Ian. *Russia accused of unleashing cyberwar to disable Estonia.* Disponível em: <https://www.theguardian.com/world/2007/may/17/topstories3.russia>. Acesso em: 09 jun. 2016

USA*, The national strategy to secure cyberspace*, 2003. Disponível em: <https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf>. Acesso em: 07 ago. 2016.

USA. *The DoD cyber strategy*. Disponível em: <http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>. Acesso em: 12 ago. 2016.

USA. *The president's budget for fiscal year 2017,* 2016. Disponível em: <https://www.whitehouse.gov/omb/budget>. Acesso em: 27 ago. 2016

WEI, MAJ Lee Hsiang. The Challenges of Cyber Deterrence. *POINTER Journal of the singapore armed forces.* Singapura: v. 41, n. 1,